Advokatrådet

ADVOKAT SAMFUNDET

Forsvarsministeriet
Holmens Kanal 42

1060 København K

· fmn@fmn.dk + pah@fmn.dk + hvs@govcert.dk

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF. 33 96 97 98
FAX 33 36 97 50

DATO: 4. marts 2014
SAGSNR.: 2014 - 455
ID NR.: 281124

Høring - over udkast til forslag til lov om Center for Cybersikkerhed samt evaluering af GovCERT-loven

Ved e-mail af 04-02-2014 har Forsvarsministeriet anmodet om Advokatrådets bemærkninger til ovennævnte udkast.

Advokatrådet har følgende bemærkninger:

1. Udkast til forslag til lov om Center for Cybersikkerhed

Formålet med det foreliggende udkast til lovforslag er at etablere et samlet lovgrundlag for Center for Cybersikkerhed og styrke centrets muligheder for at undersøge og forebygge cyberangreb. Yderligere er formålet at regulere centrets behandling af personoplysninger.

Center for Cybersikkerhed har jf. lovforslagets § 1 "*til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af*". Center for Cybersikkerhed omfatter GovCERT, der er den statslige varselstjeneste for internettrusler, MILCERT, der er varslingstjeneste for internettrusler på Forsvarsministeriets område, den nationale it-sikkerhedsmyndighed (dog varetager PET tilsvarende funktion på Justitsministeriets område), og Informationssikkerhed og beredskab på teleområdet.

Advokatrådet anerkender behovet for Center for Cybersikkerheds arbejde og funktioner og finder det hensigtsmæssig at samle lovgrundlaget for centrets organisation og funktioner. Advokatrådet finder, at udkastet overordnet er gennemarbejdet og velbegrundet.

1.1. Indgreb i meddelelseshemmeligheden

Vedrørende indgreb i meddelelseshemmeligheden (kapitel 4 i udkastet til lovforslag) noterer Advokatrådet, at lovforslaget, under visse begrænsede omstændigheder, giver mulighed for et sådant indgreb uden retskendelse. I udkastets begrundelse (punkt 3.2.) fremhæves det, at en "*(...) sådan adgang har alene til formål at klarlægge konkrete sikkerhedshændelsers karakter* (...)". Det fremhæves videre, at den foreslåede ordning er vurderet i forhold til artikel 8 i Den Europæiske Menneskerettighedskonvention, som vedrører bl.a. ret til privatliv. I denne sammenhæng fremhæves det, at formålet "*(...) ikke i sig selv er at indsamle personoplysninger. Indsamlingen er i stedet en uundgåelig konsekvens af varslingsopgaven.*". Desuden fremhæves at opbevaring af oplysninger vil være underlagt strenge sikkerhedsforanstaltninger, og det konkluderes, at forslaget opfylder betingelserne i artikel 8, stk. 2 i Den Europæiske Menneskerettighedskonvention (punkt 3.2.1.).

Samlet konkluderes det i udkastet, at indgreb i meddelelseshemmeligheden "*vil alene finde anvendelse, hvis der i forbindelse med monitoreringen af netværkskommunikation er behov for, at netsikkerhedstjenesten tilgår indhold af en kommunikation eller oplysninger om, at en sådan kommunikation har fundet sted. Center for Cybersikkerheds netværkstjeneste vil altid ud fra et proportionalitetshensyn i videst mulige omfang søge at løse opgaverne ved hjælp af data, som ikke vil kræve et indgreb i meddelelseshemmeligheden (...).*" Hvis der sker indgreb i meddelelseshemmeligheden, så vil behandling af personoplysninger ske efter bestemmelserne i lovforslagets kapitel 6 (punkt 3.2.3.).

Advokatrådet har på denne baggrund ingen bemærkninger.

1.2. Vedrørende personoplysninger

Lovforslagets kapitel 5 og 6 vedrører spørgsmål i forbindelse med behandlingen af personoplysninger. I udkastets begrundelse (punkt 3.3.) fremhæves det, at persondataloven som udgangspunkt ikke gælder for Center for Cybersikkerhed (persondatalovens § 2, stk. 11), dog er videregivelse af personoplysninger til Centret omfattet. Desuden vil Datatilsynet "*(...) for så vidt angår Center for Cybersikkerhed kunne indhente de fornødne oplysninger til afgørelse af, om et forhold falder ind under persondataloven, jf. lovens § 62, stk. 1.*" (punkt 3.3.1.).

Da persondataloven ikke gælder for Center for Cybersikkerhed har Forsvarsministeriet den 13.05.2013 udstedt retningslinjer for behandling af personoplysninger, disse bygger på principperne i persondataloven. Udkastet lægger op til, at disse retningslinjer videreføres ved lov. Udgangspunktet er her, at Centrets aktivitet også fremover ikke bør være omfattet af den almindelige persondataretlige lovgivning, men at principperne i persondatalovens bestemmelser om behandling af personoplysninger "*(...) i vidt omfang finder anvendelse på Center for Cybersikkerhed.*" (punkt 3.3.2.)

Vedrørende spørgsmål om oplysningspligter i forbindelse med personoplysninger anføres i udkastet følgende: "*Formålet med Center for Cybersikkerheds netsikkerhedstjeneste er ikke at behandle personoplysninger, men netværkstjenesten vil uundgåeligt skulle behandle personoplysninger indeholdt i pakke- og trafikdata i forbindelse med sine aktiviteter. Indsamlingen af personoplysninger er således en nødvendig del af netsikkerhedstjenestens virke, og det er Forsvarsministeriets vurdering, at opfyldelse af en oplysningspligt over for den registrerede vil være uforholdsmæssig vanskelig, ligesom behovet for at kunne begære indsigt eller gøre indsigelse er mindre fremtrædende end de administrative byrder, det vil påføre netsikkerhedstjenesten.*" (punkt 3.3.2.).

Vedrørende den øvrige del af Centrets virksomhed har Forsvarsministeriet overvejet, om der er behov for at indføre en oplysningspligt over for den registrerede. Hertil bemærkes at Centrets virksomhed "*som altovervejende hovedregel er rettet mod andre myndigheder og virksomheder. Det er derfor Forsvarsministeriets opfattelse, at der ikke på nuværende tidspunkt er behov for at indføre en oplysningspligt i forhold til fysiske personer. Samtidig finder Forsvarsministeriet dog, at der børe være mulighed for at lade persondatalovens kapitel 8-10 (om oplysningspligt over for registrerede, den registreredes indsigtsret og øvrige rettigheder, bl.a. indsigelsesret) finde anvendelse på de pågældende myndighedsområder (...).*" (punkt 3.3.2.).

På baggrund af Centrets særlige adgang til persondata på baggrund af indgreb i meddelelseshemmeligheden (se ovenfor) finder Forsvarsministeriet, at "*der fortsat bør gælde skærpede regler for analyse, videregivelse og sletning af disse data samt for sikkerhedsforanstaltninger i forbindelse med opbevaringen af og adgangen til data. På disse særlige områder bør der efter Forsvarministeriets opfattelse fortsat gælde regler, der fastsætter mere vidtgående krav end efter persondataloven, f.eks. med hensyn til sletningsfrister.*" (punkt 3.3.2.).

Vedrørende anvendelse af offentlighedsloven og forvaltningsloven mener Forsvarsministeriet, at de forskellige dele af Forsvarets Efterretningstjeneste så vidt mulig bør være underlagt samme regulering på centrale forvaltningsretlige områder, hvilket vil indebære, at offentlighedsloven ikke finder anvendelse på Center for Cybersikkerhed. Forsvarsministeriet anfører desuden, at Center for Cybersikkerhed "*kun i meget begrænset omfang træffer afgørelse i sager, der involverer fysiske eller juridiske personer (...)*" og mener ikke, at der foreligger "*væsentlige hensyn, som taler imod at center for Cybersikkerhed på samme vis som den øvrige del af Forsvaret Efterretningstjeneste undtages fra forvaltningslovens kapitel 4-6.*" (punkt 3.3.2.). Dog fremhæves det, at der vedrørende Centrets virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet samt ved Centrets behandling af anmodninger om tilslutning til sikkerhedstjenesten gøres særlige forhold gældende, som begrunder, at der i disse tilfælde bør være mulighed for at anvende offentlighedsloven og forvaltningsloven.

Samlet set indebærer forslaget, at Center for Cybersikkerhed fortsat ikke ville være omfattet af persondataloven, dog indeholder forslaget en række bestemmelser, som overfører nogle centrale principper i persondataloven til Center for Cybersikkerheds virke. Det fremhæves også, at Centrets behandling af personoplysninger skal være underlagt tilsyn af Tilsynet med Efterretningstjenester, og at der indføres særlige (strenge) regler om analyse, videregivelse og sletning af data, der behandles på baggrund af indgreb i meddelelseshemmeligheden. Forslaget indebærer yderligere, at Center for Cybersikkerhed som udgangspunkt undtages fra offentlighedsloven og forvaltningsloven. Her forudsættes det, at Centret "*i størst muligt omfang efterlever principperne i offentlighedsloven og forvaltningslovens kapitel 4-6.*". Yderligere forudsættes det, at Centret "*i alle afgørelsessager konkret vurderer, om det er muligt at anvende forvaltningslovens principper om partens aktindsigt, partshøring og begrundelse m.v.*". Tilsvarende forudsætter lovforslaget, at "*anmodninger om aktindsigt i størst muligt omfang behandles efter principperne i offentlighedsloven.*" (punkt 3.3.3.).

Advokatrådet har på denne baggrund ingen bemærkninger.

1.3. Vedrørende videregivelse

Forslaget indeholder bestemmelser om videregivelse af pakke- og trafikdata (punkt 3.5.2. og 3.5.3.). Forslaget fremhæver "*at der bør være restriktive rammer for Center for Cybersikkerheds videregivelse af data, der behandles på baggrund af indgreb i meddelelseshemmeligheden.*" Forslaget indeholder forskellige muligheder for videregivelse af trafikdata til forskellige aktører med henblik på at styrke og sikre den danske it-infrastruktur. Videregivelse af trafikdata kan også ske til andre landes netsikkerhedstjenester.

Lovforslaget viderefører også den mulighed, at politiet kan modtage pakke- og trafikdata fra Center for Cybersikkerhed ved begrundet mistanke om en sikkerhedshændelse. Advokatrådet noterer sig, at der ikke nærmere er taget stilling til det konkrete formål for videregivelse af data til politiet, og hvordan data, som er indsamlet på baggrund af et indgreb i meddelelseshemmeligheden (se ovenfor), nærmeres skal behandles i denne sammenhæng.

1.4. Øvrige aspekter af lovforslaget

Advokatrådet har også vedrørende de resterende aspekter af lovforslaget, særlig vedrørende opbevaring og sletning af data og vedrørende tilsyn, ingen bemærkninger.

2. Evaluering af GovCERT-lov

Advokatrådet har ingen bemærkninger til udkastet til Evaluering af GovCERT-loven.

Med venlig hilsen

Torben Jensen

FMN-PAH Heiberg, Peter Andreas

Fra:	Peter Hansen [pha@danskenergi.dk]
Sendt:	5. marts 2014 09:47
Til:	FMN-MYN-FORSVARSMINISTERIET
Cc:	FMN-PAH Heiberg, Peter Andreas; hvs@govcert.dk; Morten Baadsgaard Trolle
Emne:	VS: Høring - Udkast til lovforslag om Center for Cybersikkerhed og udkast til Evaluering af GovCERT-loven
Vedhæftede filer:	Høringsliste vedrørende udkast til forslag til lov om Center for Cybersikkerhed [DOK530596].pdf; Udkast til lovforslag om Center for Cybersikkerhed [DOK530616].pdf; Udkast til Evaluering af GovCERT-loven [DOK530617].pdf; Høringsbrev udkast til lovforslag om center for cybersikkerhed [DOK523366].pdf

Høring over udkast til forslag til lov om Center for Cybersikkerhed samt Evaluering af GovCERT-loven

Dansk Energi samt Branchefællesskab for Intelligent Energi har ikke bemærkninger til det foreliggende udkast til lovforslag om Center for Cybersikkerhed og evaluering af GovCERT-loven.

Dansk Energi og Branchefællesskab for Intelligent Energi vil nøje følge udmøntningen af en kommende lov om Center for Cybersikkerhed herunder en eventuel fastsættelse af nærmere regler vedrørende Center for Cybersikkerheds netsikkerhedstjeneste.

Med venlig hilsen

Peter Hansen, Dansk Energi
Morten Trolle, Branchefællesskab for Intelligent Energi

Med venlig hilsen

Peter Hansen
Chefkonsulent, civilingeniør
+45 35 300 779

Dansk Energi
Rosenørns Alle 9
1970 Frederiksberg C
+45 35 300 400

Fra: Forsvarsministeriet [mailto:fmn@fmn.dk]
Sendt: 4. februar 2014 15:54
Til: samfund@advocom.dk; amnesty@amnesty.dk; itd@itd.dk; info@shipowners.dk; Dansk Energi; info@danskerhverv.dk; difo@difo.dk; dit@dit.dk; mail@danskeadvokater.dk; regioner@regioner.dk; dt@datatilsynet.dk; di@di.dk; MikaelSjoberg@OestreLandsret.dk; itek@di.dk; cert@cert.dk; post@domstolsstyrelsen.dk; mail@finansraadet.dk; fdo@fdo.dk; secretariat@osl.dk; fvd@fvd.dk; info@humanrights.dk; tm@stofa.dk; itb@itb.dk; bestyrelse@it-pol.dk; kl@kl.dk; info@lf.dk; info@lif.dk; pi@di.dk; prosa@prosa.dk; post@vestrelandsret.dk; post@oestrelandsret.dk; secretaer.retspolitik@gmail.com; post@retssikkerheds-fonden.dk; rigsadvokaten@ankl.dk; rpch@politi.dk; info@rigsrevisionen.dk; info@digitalsikkerhed.dk; kontakt@ITprojektraad.dk; jw@teleindu.dk; um@fortconsult.dk; ro@gl.stm.dk; ro@fo.stm.dk
Emne: Høring - Udkast til lovforslag om Center for Cybersikkerhed og udkast til Evaluering af GovCERT-loven

Forsvarsministeriet

DANSK ERHVERV
BØRSEN
DK-1217 KØBENHAVN K
WWW.DANSKERHVERV.DK

T. +45 3374 6000
F. +45 3374 6080
INFO@DANSKERHVERV.DK

Forsvarsministeriet
fmn@fmn.dk
Sagsnr.: 2013/003214

5. marts 2014

Høring over udkast til forslag til lov om Center for Cybersikkerhed

Dansk Erhverv bakker op om regeringens intentioner om at øge it-sikkerheden i Danmark. I forhold til det aktuelle forslag om Center for Cybersikkerhed er retssikkerhed og demokratisk kontrol afgørende forudsætninger for, at indsatsen får den tilsigtede, positive effekt.

Generelle bemærkninger

Dansk Erhverv bakker op om lovforslagets intention om at styrke it-sikkerheden i Danmark gennem en professionel, offentlig indsats i regi af Center for Cybersikkerhed (CFCS). Styrkelse af it-sikkerheden i Danmark er en prioriteret sag for Dansk Erhverv. Dansk Erhverv mener, at Center for Cybersikkerhed kan give et reelt og vigtigt bidrag til it-sikkerheden i et samfund, der til stadighed bliver mere afhængig af en robust it-infrastruktur. Dansk Erhverv noterer sig, at lovforslaget ligger i forlængelse af tidligere regeringsbeslutning om at samle de beslægtede enheder "MIL-CERT" og "GovCERT" i een statslig netsikkerhedstjeneste, som reguleres samlet.

Dansk Erhverv finder, at der ligger nogle indbyggede udfordringer i, at arbejdet med at sikre civil infrastruktur placeres i regi af Forsvarets Efterretningstjeneste. Center for Cybersikkerhed har omfattende adgang til borgere og virksomheders kommunikation med offentlige myndigheder, bl.a. i kraft af et netværk af teknisk udstyr, som er installeret hos de fleste ministerier, og som kan analysere myndighedernes internettrafik (jf. "Evaluering af GovCERT-loven", udkast, januar 2014, side 3).

Der er afgørende, at der ikke kan drages tvivl om centrets formål om, at "opdage, analysere og bidrage til at imødegå sikkerhedshændelser" (§3). Principper om demokratisk kontrol, oplyste samtykker og gennemsigtighed skal derfor være gennemgående for centeret virke. Uklarhed om praksis kan skabe mistillid, som i sidste ende kan vanskeliggør centerets virke og stille sig i vejen for nødvendige samarbejder med bl.a. danske virksomheder. Åbenhed og kommunikation er således en vigtigt del af centerets arbejde for at fremme it-sikkerhed i Danmark.

Specifikke bemærkninger

Kapital 4 – om indgreb i meddelelseshemmeligheden: Det bør eksplicitetes, at tilslutning til CFCS altid er frivillig, og aldrig sker uden oplyst samtykke fra virksomhederne. Den nuværende

DANSK ERHVERV

/JSA
jsa@danskerhverv.dk

fremstilling i lovudkastet er ikke tilpas klar, og kan læses derhen, at tilslutning kan foregå uden virksomhederne samtykke, men alene efter vurdering internt i Center for Cybersikkerhed, så længe der er tale om en begrænset varighed på højst to måneder (§6, stk. 2 og 3).

§8 undtagelser fra persondataloven, forvaltningsloven og offentlighedsloven: Center for Cybersikkerhed er – i kraft af placeringen under Forsvarsministeriet – undtaget fra bl.a. persondataloven. Stk. 2 åbner dog mulighed for, at "Forsvarsministeren kan bestemme, at kapitel 8-10 i lov om behandling af personoplysninger, lov om offentlighed i forvaltningen samt forvaltningslovens kapitel 4-6 helt eller delvis finder anvendelse for Center for Cybersikkerhed". Det er på nuværende tidspunkt uklart, hvad dette indebærer i praksis, og hvordan det stiller borgere og virksomheder retssikkerhedsmæssigt.

Med tanke på CFCSs omfattende adgang til borgere og virksomheders kommunikation med den offentlige sektor skal Dansk Erhverv opfordre til, at forsvarsministeren benytter lovens mulighed, og definerer klare regler for håndteringen af persondata, der så vidt muligt afspejler praksis i andre offentlige myndigheder.

§16 – videregivelse af data til Forsvarets Efterretningstjeneste og andre lande: Placeringen af Center for Cybersikkerhed i Forsvarsministeriet har betydning for udveksling af data, som får karakter af "intern udveksling". Det indebærer, at "der som udgangspunkt er fri adgang til at udveksle data internt i Forsvarets Efterretningstjeneste, herunder mellem Center for Cybersikkerhed og den øvrige del af efterretningstjenesten (...)" (lovforslagets bemærkninger, side 26).

Af bemærkningerne fremgår det, at Forsvarsministeriet vil "udstede administrative retningslinjer, der sikrer, at den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste også fremadrettet sker med respekt for retssikkerheden og den personlige frihed" (side 26). Dansk Erhverv skal opfordre til maksimal åbenhed om disse administrative retningslinjer og praksisser.

Dansk Erhverv vil desuden opfordre til, at Center for Cybersikkerhed giver en årlig afrapportering, som skal være med til at skabe gennemsigtighed om centrets arbejde. Det kunne eksempelvis være relevant at oplyse om baggrunden for og antallet af (midlertidigt) tilslutninger, samt statistik på databehandlinger, sikkerhedshændelser, udvekslinger med andre myndigheder og lande m.v.

Med venlig hilsen

Janus Sandsgaard
Chefkonsulent

TELE INDUSTRIE

2. marts 2014
HEM

Forsvarsministeriet
Att.: Peter Heiberg
Holmens Kanal 42
1060 København K

Høring vedr. Lov om Center for Cybersikkerhed

DI og DI ITEK takker for henvendelsen vedrørende høring af Forslag til Lov om Center for Cybersikkerhed. DI, DI ITEK og TI har i den anledning nedenstående bemærkninger.

Positivt udgangspunkt
DI og DI ITEK er tilfredse med, at der som opfølgning på regeringsbeslutningen i 2011 om at oprette et Center for Cybersikkerhed (CFCS) under Forsvarets Efterretningstjeneste (FE) nu etableres et lovgrundlag for CFCS', herunder GovCERTs, virke (CFCS-loven). Der er tilsvarende tilfredshed med, at der i samme forbindelse etableres et lovgrundlag for MIL-CERTs virke, som tidligere har været ureguleret.

På de overordnede linjer er vi også meget tilfredse med, at væsentlige dele af reguleringen af CFCS' virke tager udgangspunkt i og viderefører en række principper fra den eksisterende "Lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v." (GovCERT-loven), der med det nye forslag til CFCS-loven ophæves.

Endelig er vi tilfredse med, at analysen af de pakkedata, som CFCS' prober opsamler i civile netværk, jf. CFCS-lovens §4, efter CFCS-lovens § 15 kun må "finde sted ved begrundet mistanke om en sikkerhedshændelse og kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen", svarende til bestemmelsen i GovCERT-lovens §4, stk. 1. Denne bestemmelse giver en fornuftig begrænsning i forhold til behandling af personoplysninger.

Forholdet til persondataloven
GovCERT-lovens §5 præciserede, at GovCERT-funktionen alene var undtaget persondatalovens §35, mens det nye CFCS med sin placering under FE generelt er undtaget hele persondataloven, jf. CFCS-loven §8, stk. 1 og persondataloven §2, stk. 11.

I lyset af at GovCERT gennem sine prober på nuværende tidspunkt har adgang til betydelige dele af kommunikationen mellem borgerne/virksomheder og staten og på længere sigt får adgang til stadig større dele af kommunikation mellem borger/virksomheder og brede dele af den offentlige sektor m.v. og især i lyset af at ovenstående adgang gives som følge af en proportionalitetsafvejning mellem Grundlovens §72 (indgreb i meddelelseshemmeligheden) og EMRK artikel 8 (retten til privatlivets fred) på den ene side og de samfunds-

Postadresse/Postal address
1787 København V
Danmark
(+45) 3377 3377
itek@di.dk
itek.di.dk
Besøgsadresser/Visiting addresses
Hannemanns Allé 25
København S
Sundkrogskaj 20
København Ø
CVR: 16 07 75 93

mæssige interesser i at håndtere sikkerhedshændelser for offentlige myndigheder på den anden side, og endelig i lyset af den udvidelse af datagrundlaget der lægges op til, herunder særligt mulighederne for at bryde fortrolig krypteret kommunikation (jf. nedenfor), synes det at være en udfordring i forhold til at beskytte borgernes og virksomhedernes retssikkerhed at undtage al denne kommunikation fra den beskyttelse, som persondataloven giver.

I henhold til den evaluering af GovCERTs virke, som Forsvarsministeren skal give Folketinget i henhold til GovCERT-lovens §9, og som foreligger i udkast her i januar 2014, synes der ikke at have været fagligt behov for at udvide undtagelserne fra persondataloven.

Forsvarsministeriet har, for at råde bod på den væsentlige ændring af anvendelsen af persondataloven i GovCERTs virke, dels indarbejdet §§ 9-14 og §18 i CFCS-loven og dels indraget en række af principperne fra persondataloven i Forsvarsministeriets "Retningslinjer for behandling af personoplysninger m.v. i Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste" (Retningslinjer af 13. maj 2013). Således kan der siges at være et betydeligt sammenfald mellem persondataloven, retningslinjerne af 13. maj 2013 og CFCS-loven som følger:

Persondataloven	Retningslinjerne af 13. maj 2013	CFCS-loven
§3 (definitioner)	§2	
§5 (god behandlingsskik)	§10	§9, §13 og §14
§6 (almindelige oplysninger)	§11	§10
§7 (følsomme oplysninger)	§12	§11
§8 (rent private forhold)	§13	§12
§41 (sikkerhed)	§14	§18 (uden krigsreglen)

Retningslinjerne af 13. maj 2013 bliver efter lovens ikrafttræden erstattet af nye retningslinjer, hvis indhold vi ikke kender. Retningslinjerne kan desuden alene anvendes til tjenestelige sager og kan ikke bruges af en domstol.

Det er et positivt skridt, at Forsvarsministeriet lægger op til, at CFCS skal følge persondataloven på så væsentlige punkter. Det er også et naturligt skridt, at visse dele af persondataloven ikke finder anvendelse for CFCS, f.eks. §§ 15-26 om kreditoplysningsbureauer og §§ 43-54 om anmeldelse til Datatilsynet.

Imidlertid synes det bemærkelsesværdigt at:

1. krigsreglen (Retningslinjerne af 13. maj 2013, §14, stk. 3 og persondataloven §41, stk. 4) ikke finder vej til CFCS-loven
2. der ikke lægges op til at spørge eller i det mindste orientere Tilsynet med Efterretningstjenesterne i principielle sager hvor der behandles personoplysninger, jf. f.eks. persondataloven §7, stk. 7
3. der ikke lægges op til at give borgere og virksomheder et lille minimum af rettigheder i henhold til persondatalovens §§ 28-40.

Der opfordres til, at Forsvarsministeren anvender sin mulighed i CFCS-loven §8, stk. 2 og vurderer, om det er muligt at tildele borgere og virksomheder et minimum af rettigheder.

Der opfordres desuden til at bruge Tilsynet som vejledende organ og til at implementere krigsreglen.

Udvidelse af datagrundlaget begrænser konkurrencen
Datagrundlaget for GovCERT var bestemt ved GovCERT-lovens §4, stk. 1, hvor det omfattede: "tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata". Med CFCS-loven lægges der op til, at datagrundlaget udvides på fem forskellige måder.

Den første udvidelse af datagrundlaget sker som følge af at mængden af organisationer, som kan tilslutte sig CFCS netsikkerhedstjeneste, bliver udvidet, når man ændrer ordlyden fra "kritisk infrastruktur" (GovCERT-lovens §2) til "samfundsvigtige funktioner" (CFCS-lovens §1).

Med denne udvidelse af datagrundlaget er der en risiko for, at CFCS netsikkerhedstjeneste kommer i konkurrence med private sikkerhedsleverandører. I "bemærkninger til lovforslagets enkelte bestemmelser" præciseres det, at de samfundsvigtige funktioner omfatter: "sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet... medicinalvirksomheder, fødevarevirksomheder, virksomheder, der leverer vigtige komponenter til Forsvaret, og virksomheder, der varetager driften af administrative it-systemer for det offentlige" (p. 35).

Listen viser, at en ganske stor del af det private erhvervsliv kan tilslutte sig CFCS netsikkerhedstjeneste. Dermed kan netsikkerhedstjenesten gå i direkte konkurrence med private udbydere af sammenlignelige services. Der findes på det private marked tjenester, der i et vist omfang er sammenlignelige med CFCS netsikkerhedstjeneste. Flere sikkerhedsvirksomheder har f.eks. et system af prober til at opsamle data og analysere sikkerhedshændelser på det globale internet, svarende til hvad CFCS netsikkerhedstjeneste har på den danske del af internettet. De pågældende virksomheder har selv status af at være CERTer eller CSIRTer og indgår derfor CERT-CC samarbejdet med deres data. At være i konkurrence med sådanne virksomheder synes ikke at være foreneligt med CFCS formål.

DI, DI ITEK og TI mener derfor, at det bør præcises i lovens bemærkninger, at CFCS's aktiviteter bør tilrettelægges således, at netsikkerhedstjenesten mindst muligt konkurrer med private udbydere af sammenlignelige services.

Der er omvendt begrænsninger på, hvem der kan tilslutte sig CFCS' netsikkerhedstjeneste, og disse begrænsninger fastlås det i loven, at CFCS selv skal være herre over. I "bemærkninger til lovforslagets enkelte bestemmelser" uddybes kriterier for at en virksomhed kan tilsluttes: "[virksomhederne skal] kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet" og at "netsikkerhedstjenesten samlet set opnår en samfundsmæssigt repræsentativ dækning" (p. 36). Det betyder, at den første medicinalvirksomhed, som tilmelder sig tjenesten godt kan blive optaget, men den næste medicinalvirksomhed, kan ikke blive tilsluttet. Skulle det ske, at CFCS opdager en sikkerhedshændelse indenfor medicinalindustrien, kan den første virksomhed altså blive bedre stillet end de øvrige.

CFCS bør i loven pålægges, at i det omfang, de opdager sikkerhedshændelser, der er målrettet enkelte virksomheder eller sektorer, har CFCS en forpligtelse til at orientere den enkelte virksomhed eller sektorens brancheorganisation med relevante informationer om angrebet uanset om virksomheden eller sektoren er tilsluttet CFCS eller ej.

Den anden udvidelse af datagrundlaget sker, når man udvider netsikkerhedstjenesten til foruden af omfatte data fra GovCERT også omfatter data fra MILCERT. DI, DI ITEK og TI har ingen bemærkninger til denne udvidelse af datagrundlaget.

Den tredje udvidelse af datagrundlaget sker, når man åbner op for, at virksomheder og myndigheder midlertidigt kan tilsluttes netsikkerhedstjenesten i henhold til CFCS-lovens §6. Den fjerde udvidelse af datagrundlaget sker, når der er behov for at analysere data fra et informationssystem i henhold til CFCS-lovens §7. Hvad angår håndtering af sådanne pludseligt opståede sikkerhedshændelser, findes der en lang række af private aktører, som allerede påtager sig at levere sådanne services på markedsvilkår. At være i konkurrence med sådanne virksomheder synes ikke at være foreneligt med CFCS formål. Vi anbefaler derfor, at CFCS henviser til private leverandører, når der skal foretages arbejde afledt af midlertidig tilslutning efter §6, og når der skal analyseres informationssystemer efter §7.

Iøvrigt fremgår det ikke klart af loven, om den midlertidige tilslutning og analyse af data fra et informationssystem er noget, som er frivilligt for den som er ramt af en sikkerhedshændelse, eller om CFCS har myndighed til at pålægge en juridisk person, som CFCS mener har været udsat for en sikkerhedshændelse, at blive tilsluttet eller få analyseret sit informationssystem. Det bør præciseres i bemærkningerne, at samtykket i CFCS-loven §6, nr. 1 og §7, nr. 1 betyder at både midlertidig tilslutning og analyse af data fra et informationssystem er frivilligt, og ikke kan pålægges af CFCS.

Den femte udvidelse af datagrundlaget sker i og med at GovCERT ikke havde hjemmel til at bryde kryptering, men at CFCS får denne hjemmel (bemærkninger til lovforslagets enkelte bestemmelser, p. 37). DI, DI ITEK og TI anerkender, at kriminelle ofte anvender kryptering for at skjule deres handlinger. Det forhold bør dog afvejes imod at borgere og virksomheder ofte også bruger kryptering til at særligt fortrolige data, og at CFCS derfor ved at bryde krypteringen må forvente at få adgang til data, som er endnu mere følsomme end hidtil. Det er vigtigt, at man fra politisk hold er opmærksom på denne afvejning.

Videregivelse af data til teleselskaberne

Med CFCS-lovens §16 lægges der op til at udvide videregivelse af forskellige data til forskellige parter. Videregivelse af trafikdata kan i henhold til stk. 2 bl.a. ske til "udbydere af offentlige elektroniske kommunikationsnet og –tjenester". I "bemærkninger til lovforslagets enkelte bestemmelser" p. 44 hedder det, at "især teleselskaber kan forbedre deres sikkerhedssystemer, således at den ikt-infrastruktur, som samfundsvigtige funktioner i overvejende grad er afhængige af, kan sikres yderligere". Formuleringen rejser spørgsmålet om, hvem der har ansvaret for brugen af informationerne. Konkret vil CFCS formodentlig levere en række IP-adresser, som indeholder skadelige services - f.eks. command and controlservere eller dropservere i BOT-nets - til teleselskaberne og ved samme lejlighed fremsætte et ønske om, at de pågældende IP-adresser blokeres. Loven placerer imidlertid ikke et ansvar for blokeringen, og det betyder, at hvis teleselskaberne efterkommer CFCS

ønske, så kan teleselskaberne risikere at hænge på regningen og dårlig omtale ved at bedrive censur af tjenester på internettet og lege politimand på CFCS' vegne. Når §16, stk. 2 så ses i sammenhæng med §17, stk. 4, hvor det fremgår, at CFCS ikke pålægger en sletteplig ved videregivelse af data i medfør af §16, stk. 2, står teleselskaberne i en situation, hvor de ikke ved, hvornår blokeringen af de omtalte IP-adresser skal ophøre, og altså risikerer at holde tjenester på nettet blokeret længere end nødvendigt.

DI, DI ITEK og TI mener, at det er ganske udmærket, at loven ikke forhindrer, at CFCS netsikkerhedstjeneste kan videregive trafikdata til teleselskaberne. Men skal man få succes med dette tiltag og gøre en reel forskel for at beskytte samfundsvigtige funktioner gennem blokering, er det vigtigt, at loven præciserer, at ansvaret for blokeringen ligger hos CFCS, og at CFCS har en forpligtelse til at angive, i hvilket tidsrum blokeringen skal opretholdes. Det bør desuden overvejes at kompensere teleselskaberne for den økonomiske byrde, det vil være at implementere og fjerne blokeringen.

Videregivelse af data fra GovCERT til MILCERT og FE
I GovCERT-loven §6, stk. 2 hed det: "Pakkedata, der knytter sig til en sikkerhedshændelse, kan videregives til Forsvarets Efterretningstjenestes militære CERT, hvor IT- og Telestyrelsen skønner det nødvendigt for at beskytte nationale digitale infrastrukturer mod sikkerhedsmæssige trusler". CFCS har gentagne gange understreget, at netop opretholdelsen af dette forhold er det, som sikrer borgernes retssikkerhed.

Med CFCS-loven fjernes denne beskyttelse: "En sådan intern udveksling af data har efter oprettelsen af Center for Cybersikkerhed ikke længere karakter af en videregivelse, og den interne udveksling af data i Forsvarets Efterretningstjeneste er... ikke længere reguleret i lovforslaget" (almindelige bemærkninger, p. 26). I udgangspunktet betyder det, at FE i bred forstand får adgang til GovCERTs data (også pakkedata), og FE kan derfor i udgangspunktet bruge disse data, indenfor de rammer der er bestemt i FE-loven. Det synes at være en ganske vid udvidelse i anvendelsen af data, ikke mindst fordi det som tidlige anført handler om al kommunikation mellem borgere/virksomheder og den offentlige sektor m.v.

I bemærkningerne, p. 9, hedder det også om Retningslinjerne af 13. maj 2013, at: "Retningslinjerne fastsætter derudover en række bestemmelser om den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste". Retningslinjerne erstattes af nye retningslinjer efter CFCS-lovens vedtagelse. Hvis det kan lægges til grund at indholdet af retningslinjerne vil blive videreført, således som de almindelige bemærkninger (p. 26) indikerer: "Forsvarsministeriet vil imidlertid med lov om Center for Cybersikkerheds ikrafttræden udstede administrative retningslinjer, der sikrer, at den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste også fremadrettet sker med respekt for retssikkerheden og den personlige frihed", så gælder det jf. §6, stk. 2, at "Vurderingen af, om en videregivelse af trafikdata til FE's efterretningsmæssige virksomhed er nødvendig i henhold til varslingstjenestens formål og aktiviteter, jf. GovCERT-lovens §6, nr. 3, foretages af chefen for CFCS eller en af denne udpeget person"..

DI, DI ITEK og TI mener, at det er uklart, i hvilket omfang GovCERTs data kan bruges af FE. Vi mener også, at det er en uheldig konsekvens af CFCS placering i FE, at der er risiko for at der bliver en så vid adgang til GovCERTs data. Vi anbefaler, at:

- at det i de kommende retningslinjer fortsat fastslås, at der fra gang til gang skal tages stilling til, om pakkedata kan videregives fra CFCS til FE
- at adgang for FE kun må gives, når det er nødvendigt i henhold til CFCS's formål og aktiviteter eller der foreligger et andre nærmere kvalificerede beskyttelsesværdige formål,
- at det overordnet sikres, at der ikke sker et automatisk og generelt flow af alle trafikdata fra GovCERT til FE

Videregivelse af data til udlandet

I CFCS-lovens §16, nr. 2 hedder det, at: "trafikdata videregives til... andre netsikkerhedstjenester". Dette uddybes i de almindelige bemærkninger (p. 25) med, at det er en forudsætning for CFCS succes, at trafikdata kan videregives til andre landes CERTer og iktsikkerhedsmyndigheder.

Vi noterer os med tilfredshed, at pakkedata alene må videregives til politiet jf. §16, nr. 1. Vi finder det samtidig absolut nødvendigt med et samarbejde mellem myndighederne på tværs af grænser, idet langt størsteparten af den it-kriminalitet der foregår, er grænseoverskridende. Da §16, nr. 2 henviser til data der er omfattet af §§ 4, 6 og 7 synes der ikke at være nogen begrænsning på omfanget af trafikdata, som kan videregives til udlandet. Basalt set ville alle indsamlede trafikdata kunne overføres til samarbejdspartnere i fremmede lande. I lyset af den udvidelse af datagrundlaget, der med lovforslaget finder sted, synes det rimeligt, at sikre en vis begrænsning i mulighederne for at overføre data eller i det mindste at underlægge omfanget demokratisk kontrol. DI, DI ITEK og TI anbefaler konkret, at der kun må overføres trafikdata til udlandet, som er tilknyttet en sikkerhedshændelse som defineret i §2, nr. 1. Alle trafikdata, som ikke er tilknyttet en sikkerhedshændelse, må dermed ikke overføres.

Slettefrister

Med CFCS-loven ændres der betydeligt i slettefristerne. Trafik- og pakkedata behandles nu ens. Det betyder, at pakkedata, hvortil der ikke er knyttet en sikkerhedshændelse, nu kan gemmes i 13 måneder (CFCS-loven, §17, stk. 2) i modsætning til tidligere i 14 dage (GovCERT-loven, §4, stk. 3, nr. 2). Trafikdata, hvortil der ikke er sket en sikkerhedshændelse, kan gemmes i 13 måneder mod tidligere 12 måneder.

Yderligere slås det i CFCS-loven, §4, stk. 4 fast, at der ikke stilles krav om sletning for data, som videregives.

Sammenholdes bestemmelserne om videregivelse til udlandet og slettefristerne står der basalt set i loven, at alle trafikdata kan videregives til udlandet og aldrig behøver at blive slettet.

DI, DI ITEK og TI finder det ikke proportionalt, at pakkedata kan gemmes i 13 måneder og foreslår, at tidshorisonten sænkes til én måned. Desuden synes det ikke rimeligt, at der ikke stilles krav om sletning, når data videregives. Dette gælder både videregivelse af trafikdata til teleudbyderne (jf. bemærkningerne ovenfor) og ved videregivelse til myndighe-

der i udlandet. Derfor anbefaler vi, at der når data videregives, fastsættes krav om sletning.

Tilsynet
I lyset af placeringen af CFCS i FE er det naturligt at nedlægge Tilsynet med GovCERT og overlade opgaven til Tilsynet med Efterretningstjenesterne.

Tilsynet med GovCERT skulle i henhold til GovCERT-loven §7, stk. 2 kunne præstere juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab. Tilsynet med CFCS bliver i henhold til CFCS-loven, kapitel 9, Tilsynet med Efterretningstjenesterne. Men i PET-lovens kapitel 9 findes der ikke tilsvarende krav til sagkundskaben hos dem, der udpeges til Tilsynet. Der er derfor en risiko for, at man vil mangle kompetencer i det nye tilsyn.

Det bør sikres, at Tilsynet med Efterretningstjenesterne har adgang til den fornødne sagkundskab og ikke alene repræsenterer juridiske kompetencer.

Andre bemærkninger
I CFCS-loven §17, stk. 3 omtales registrering af data. Registrering defineres ikke noget sted i loven. I den konkrete situation er der dermed en risiko for, at CFCS kan have data liggende, som ikke er registrerede, og dermed ikke er omfattet af slettefristerne. I et bredere perspektiv kunne der også være en risiko for, at sådanne data slet ikke er omfattet af loven. Det bør i bemærkningerne præciseres, at en registrering i overensstemmelse med det persondataretlige begreb er en behandling jf. CFCS-lovens § 2, nr. 5.

I både "Evaluering af GovCERT-loven" og lovforslagets almindelige bemærkninger 3.2.2 fremhæves vigtigheden af adgang til pakkedata. Imidlertid vil det være nyttigt, dersom der mere generelt bliver fremlagt vurdering af CFCS effektivitet med hensyn til at efterleve formålet i CFCS-lovens §1. Vi opfordrer til, at CFCS offentligt demonstrerer, at de faktisk har en effekt på cybersikkerheden i Danmark.

For at sikre, at formålet med CFCS kan opfyldes er det nødvendigt, at CFCS får informationer fra de tilsluttede virksomheder enten i form af CFCS anmoder om oplysningerne eller virksomheden af egen drift informere CFCS om forhold der er kan understøtte et højt informationssikkerhedsniveau i samfundet eller virksomheden har en mistanke om en sikkerhedshændelsen. Loven synes imidlertid alene at vedrører den behandling af oplysninger Center for Cybersikkerhed kan foretage. Selve udleveringen af personoplysning herunder trafik- og pakkedata der sker på initiativ af en privat virksomhed er derimod ikke behandlet i loven. Da en sådan udlevering af oplysninger ikke nødvendigvis er lovlig efter hhv. persondataloven eller teleloven, bør det præciseres i CFCS-loven, at udleveringen af personoplysning herunder trafik- og pakkedata til CFCS lovlig kan foretages af en tilsluttet virksomhed uden at der foreligger en konkret anmodning fra CFCS.

Vi står naturligvis til rådighed med en uddybelse af ovenstående synspunkter.

Med venlig hilsen

Henning Mortensen
Chefkonsulent
DI ITEK

Jakob Willer
Direktør
Teleindustrien

DATATILSYNET

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt til: fmn@fmn.dk med kopi til
pah@fmn.dk og hvs@govcert.dk

3. marts 2014

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2014-112-0304
Sagsbehandler
André Dybdal Pape
Direkte 3319 3223

Vedrørende høring over udkast til forslag til lov om Center for Cybersikkerhed samt evaluering af GovCERT-loven

Ved brev af 4. februar 2014 har Forsvarsministeriet sendt ovennævnte udkast og anmodet om Datatilsynets eventuelle bemærkninger hertil.

Udkastet giver ikke umiddelbart Datatilsynet anledning til bemærkninger.

Med venlig hilsen

André Dybdal Pape

DEN DANSKE DOMMERFORENING

Dato: 21. februar 2014

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt pr. mail til fmn@fmn.dk, pah@fmn.dk og hvs@govcert.dk

Forsvarsministeriet har ved brev af 4. februar 2014 (Sagsnr. 2013/003214) anmodet Dommerforeningen om eventuelle bemærkninger til forslag til høring over udkast til forslag til lov om Center for Cybersikkerhed samt Evaluering af GovCERT-loven.

I den anledning skal jeg meddele, at udkastet ikke giver Dommerforeningen anledning til at fremkomme med bemærkninger.

Med venlig hilsen

Mikael Sjöberg

Formanden, Østre Landsret, Bredgade 59, 1260 København K, tlf. 99 68 65 01
mikaelsjoberg@oestrelandsret.dk

DeiC
DANISH E-INFRASTRUCTURE COOPERATION

Forsvarsministeriet
Holmens Kanal 42
1060 København K
Att.: Peter Heiberg

4. marts 2014

Høring vedr. udkast til lovforslag om Center for Cybersikkerhed

DKCERT har haft forslag til lovgrundlag for Center for Cybersikkerheds aktiviteter til gennemsyn for en kommentar. DKCERT takker for denne mulighed for at give udtryk for vores holdning til den fremtidige behandling af sikkerhedshændelser i Danmark.

DKCERT har lang tids erfaring med at bekæmpe internet-relateret kriminalitet for borgerne i almindelighed og for Forskningsnettet i særdeleshed. DKCERT har siden 1991 været en del af det danske it-sikkerhedsbillede, først i undervisningssektoren som en del af UNI-C og siden 1. januar 2013 i forskningsverdenen som en del af DeIC, Danish e-Infrastructure Cooperation, og DTU, Danmarks Tekniske Universitet. DKCERT har været meget tilfreds med samarbejdet med statslige it-sikkerhedsmyndigheder og ser frem til at fortsætte denne positive linje.

Det er i denne egenskab af samarbejdspartner på it-sikkerhedsområdet, at vores bidrag til høringen omkring lovforslaget skal ses: som en aktiv part i forebyggelse, behandling og efterforskning af sikkerhedshændelser på nettet. Vi opfatter det nye Center for Cybersikkerheds nettjenester som en samarbejdspartner, der kan medvirke til at hæve DKCERTs informationsniveau. Dermed kan centeret sætte DKCERT i stand til at servicere vores kernekunder i forskningsverdenen samt andre kunder i erhvervsliv og det civile samfund på den bedst tænkelige måde ved at lade os løse presserende sikkerhedsopgaver. En hurtig og konsekvent indgriben til fordel for vores kunder vil altid være vores første prioritet, understøttet af varslinger og gode råd om, hvordan man skal højne bevidstheden om it-sikkerhed.

På denne baggrund har vi følgende at bemærke til det nye lovforslag:

1) DKCERT ser positivt på lovforslaget som grundlag for en ny og centraliseret organisation til at tage vare på den nationale sikkerhed i Danmark. Vi ser det som et skridt til at opdatere lovgrundlaget til at afspejle en ny virkelighed, og i forlængelse heraf til en mere effektiv behandling af sikkerhedshændelser, som vedrører det danske samfund.

2) DKCERT ser som samarbejdspartner positivt som på enhver mulighed for at videregive sikkerhedsrelaterede informationer, herunder videregivelser som er undtaget krav til retskendelser, undtaget persondataloven og forvaltningsloven i overensstemmelse med den nye

DeIC Sekretariat
Danmarks Tekniske Universitet, Anker Engelunds Vej 1, Bygning 101A, 2800 Kgs. Lyngby.
Telefon 45 25 72 64 * Mail: sekretariat@deic.dk * website: www.deic.dk * EAN: 5798000430723

DeiC

DANISH e-INFRASTRUCTURE COOPERATION

organisations placering under Forsvarsministeriet. Vi anerkender, at samfundets overordnede interesse nu er lagt som kriterium for registrering og behandling.

3) DKCERT mener, at udvidelsen af dækningsområdet og introduktionen af midlertidigt tilsluttede virksomheder og institutioner principielt set er begrundet. DKCERT finder, at det her vil være mere produktivt, hvis der etableres et formaliseret samarbejde, idet der er tale om nogen grad af overlappende indsatsområder. Vi anbefaler derfor et formaliseret samarbejde, hvori DKCERT som Forskningsnettets CERT (Computer Security Incident Response Team) skal indarbejdes som privilegeret samarbejdspartner, hvor informationer kan udveksles i it-sikkerhedens interesse.

4) DKCERT er enig i, at en udvidelse af betingelserne for at slette data med og uden tilknytning til sikkerhedshændelser til maksimalt 13 måneder for både pakke- og trafikdata vil være med til at effektivisere bekæmpelsen af internetrelateret kriminalitet.

5) Muligheden for at videregive trafikinformationer til andre netsikkerhedstjenester ser DKCERT som et nødvendigt redskab til at forbedre det internationale samarbejde.

6) DKCERT tiltræder derfor også, at rammerne omkring forebyggende og efterforskende aktiviteter skal ligestilles, for at indsatsen kan være så proaktiv så muligt i kampen for en bedre sikkerhed.

7) DKCERT finder, at nævnte sammenlægning og organisatoriske placering retfærdiggør organisering af et tilsyn, som er gearet til den nye organisation. Vi finder, at den udvidede tilsynsorganisation kan udøve sin funktion på betryggende vis.

Med venlig hilsen

Shehzad Ahmad
DKCERT (DeIC, DTU)

DeIC Sekretariat
Danmarks Tekniske Universitet, Anker Engelunds Vej 1, Bygning 101A, 2800 Kgs. Lyngby.
Telefon 45 25 72 64 * Mail: sekretariat@deic.dk * website: www.deic.dk * EAN: 5798000430723

Domstolsstyrelsen

Store Kongensgade 1-3
1264 København K
Tlf. +45 70 10 33 22
Fax +45 70 10 44 55
post@domstolsstyrelsen.dk
CVR nr. 21-65-95-09
EAN-nr.5798000161184

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendes med e-mail til fmn@fmn.dk med kopi til pah@fmn.dk og hvs@govcert.dk

J. nr. 2014-4102-0008-3

Sagsbeh. Katrine V Trebbien
Dir.tlf. + 45 99 68 42 43
Mail kat@domstolsstyrelsen.dk

Høring over udkast til forslag til lov om Center for Cybersikkerhed samt Evaluering af GovCERT-loven

4. marts 2014

Forsvarsministeriet har ved brev af 4. februar 2014 sendt udkast til forslag til lov om Center for Cybersikkerhed samt udkast til evaluering af GovCERT-loven i høring.

Domstolsstyrelsen har ingen bemærkninger til de to udkast.

Med venlig hilsen

Niels Juhl

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Høringssvar til lovforslag om Center for Cybersikkerhed og evaluering af GovCERT-loven

Ved brev den 4. februar 2014 har forsvarsministeriet sendt lovforslag om Center for Cybersikkerhed samt evaluering af GovCERT-loven i officiel høring og anmodet om Finansrådets bemærkninger.

Finansrådet bifalder beslutningen om at etablere et statsligt Center for Cybersikkerhed i Danmark, og det glæder bankerne at se den øgede fokus på it-sikkerhed i Danmark, som er væsentlig for kriminalitetsbekæmpelse i takt med, at internettet spiller en stadig større rolle i samfundet.

Finansrådet har følgende bemærkninger til lovforslaget:

Ad § 3, stk. 3
I forhold til den opgave, Center for Cybersikkerhed skal varetage, henledes opmærksomheden på segmentet af virksomheder, som ikke er kritiske for Danmarks infrastruktur, men hvor sikkerheden alligevel kan være afgørende. En del vira spredes igennem udbydere af hjemmesider, der eksempelvis uden viden herom har en virusinficeret annonce liggende på hjemmesiden. Der savnes et sted at sende sådanne sager hen, idet det lige nu ikke er omfattet af de forskellige CERTer. Hvor kan en mindre virksomhed gå hen for råd og vejledning, og hvortil kan sikkerhedstjenester, der bliver opmærksomme på inficerede sider, overdrage denne viden? Dette vil bankerne gerne have afklaret.

Ad § 16, stk. 1, nr. 1
I forbindelse med videregivelse af oplysninger til efterforskning er bankernes erfaring, at det ikke altid er muligt at spore en kriminel handling via ISP'erne med en IP-adresse. Anvendelsen af IP-adresserne har ændret sig, og tildelingen via NAT (Network Address Translation) enheder muliggør tilslutning af flere enheder til internet med den samme offentlige IP-adresse. Bankerne opfordrer derfor til en dialog med ISPer for at sikre sporbarhed. Dette kan sikres, hvis ISPerne overholder BCP38 (best current practice nr. 38), der stiller krav til, at teleudbydernes netværk er "rent", dvs. at der ikke er falske (spoofede) adresser.

Med venlig hilsen

Henriette Rolskov
Direkte +45 3370 1102
her@finansraadet.dk

4. marts 2014

Finanssektorens Hus
Amaliegade 7
1256 København K

Telefon 3370 1000
Fax 3393 0260

mail@finansraadet.dk
www.finansraadet.dk

Journalnr. 466/01
Dok. nr. 517393-v1

FMN-PAH Heiberg, Peter Andreas

Fra: Anette Høyrup [ah@fbr.dk]
Sendt: 5. marts 2014 11:20
Til: FMN-PAH Heiberg, Peter Andreas; hvs@govcert.dk
Cc: FMN-MYN-FORSVARSMINISTERIET
Emne: Høringssvar vedr. Center for Cybersikkerhed
Vedhæftede filer: 20140304 RfDS høringssvar CFCS.pdf

Til Forsvarsministeriet
Att.: Peter Heiberg

Forbrugerrådet Tænk har ikke været på høringslisten vedrørende ovennævnte lovforslag, men vi gør hermed opmærksom på, at vi på linje med mange andre organisationer i Danmark, står bag vedhæftede høringssvar af g.d. fra Rådet for Digital Sikkerhed.

Med venlig hilsen

Anette Høyrup
Seniorjurist / Senior Legal Adviser

T +45 7741 7738 / M +45 2715 7432 / taenk.dk
Fiolstræde 17 B / Postboks 2188 / 1017 København K

Forbrugerrådet
Tænk
Danish Consumer Council

INSTITUT FOR MENNESKE RETTIGHEDER

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
DIREKTE 3269 8805
RFJ@HUMANRIGHTS.DK
MENNESKERET.DK

J. NR. 540.10/30403/RFJ/MAF

Forsvarsministeriet
fmn@fmn.dk
pah@fmn.dk
hvs@govcert.dk

4. MARTS 2014

HØRING OVER UDKAST TIL FORSLAG TIL LOV OM CENTER FOR CYBERSIKKERHED SAMT EVALUERING AF GOVCERT-LOVEN

Forsvarsministeriet har ved e-mail af 4. februar 2014 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til høring over udkast til forslag til lov om Center for Cybersikkerhed samt evaluering af GovCERT-loven.

Med udkast til forslag til lov om Center for Cybersikkerhed etableres et samlet lovgrundlag for Center for Cybersikkerhed. Lovforslaget er baseret på en evaluering af den statslige varslingstjeneste for internettrusler (GovCERT), som varetages af Center for Cybersikkerhed. Evalueringen er foretaget af Forsvarsministeriet, men det fremgår ikke tydeligt af evalueringen eller lovforslaget, hvordan evalueringen er foretaget eller hvem, der er blevet hørt. Det fremgår dog, at tilsynet for GovCERT, som blev nedsat i september 2013 endnu ikke har afgivet sin første beretning, og derfor ikke har været en del af evalueringen. I evalueringen konkluderes det, at GovCERT har bidraget væsentligt til cybersikkerheden i Danmark, men at der samtidig er behov for at revidere lovgrundlaget for GovCERT, for at sikre GovCERTs evne til at bidrage til sikringen mod væsentlige angreb mod danske interesser.

Instituttet har følgende bemærkninger:

Instituttet finder det positivt at lovforslaget etablerer en lovregulering af Center for Cybersikkerhed, GovCERT og varslingstjenesten for internettrusler på forsvarsministeriets område (MILCERT). Instituttet finder endvidere, at forebyggelse af cyberangreb er et tungtvejende hensyn for danske myndigheder og virksomheder.

1. KORT OM MENNESKERETTEN

Retten til et beskyttet privatliv og familieliv reguleres bl.a. i Den Europæiske Menneskerettighedskonventions artikel 8 (EMRK) og i FN's konvention om borgerlige og politiske rettigheder (ICCPR), artikel 17. Artikel 7 og 8 i EU's charter om grundlæggende rettigheder beskytter henholdsvis retten til respekt for privatliv og familieliv og beskyttelse af personoplysninger.

EMRK art. 8 har følgende ordlyd:
"Stk.1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.
Stk. 2. Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder."

Videregivelse og anden behandling af oplysninger om enkeltpersoners private forhold, hører ind under beskyttelsesområdet i artikel 8. Statens mulighed for at foretage indgreb i retten til respekt for privatliv forudsætter opfyldelsen af tre indgrebsbetingelser, som er hjemmel i national ret, forfølgelsen af et anerkendelsesværdigt formål og et krav om nødvendighed i et demokratisk samfund.

Ved kravet om, at et indgreb skal være nødvendigt i et demokratisk samfund søges det sikret, at der består en rimelig balance i afvejningen mellem borgerens og samfundets interesser. Derudover følger det af nødvendighedskravet, at et indgrebs begrundelse skal findes i et påtrængende samfundsmæssigt behov. Undersøgelsen af, om nødvendighedskravet er opfyldt, skal suppleres af en proportionalitetsvurdering. Denne vurdering skal skabe sikkerhed for, at indgreb foretages med et middel, der må anses for proportionalt i forhold til målet, dvs. at det middel, der bringes i anvendelse, skal stå i et rimeligt forhold til det mål, som søges opnået.

EU's Persondatadirektiv (95/46/EC), fastsætter rammer for behandling af personoplysninger. Artikel 8 i direktivet fastsætter som udgangspunkt et forbud mod behandling af personoplysninger. Dette udgangspunkt kan dog fraviges, hvis den, som oplysninger vedrører, giver samtykke til behandlingen, ligesom der oplistes andre situationer, hvor udgangspunktet kan fraviges, se herved artikel 8, stk. 3. Direktivet er implementeret ved den danske persondatalov.

2. ORGANISATORISK PLACERING AF GOVCERT

Da lovgivningen, som regulerer GovCERT, blev vedtaget, var GovCERT en del af den daværende IT- og Telestyrelse under det daværende Videnskabsministerium (nu Uddannelses- og Forskningsministeriet) Ved kongelig resolution af 3. oktober 2011 blev ressortansvaret for GovCERT overført til Forsvarsministeriet og med oprettelsen af Center for Cybersikkerhed den 18. december 2012 blev GovCERT en del af Forsvarets Efterretningstjeneste. Placeringen under Forsvarets Efterretningstjeneste betyder, at GovCERT ikke er omfattet af persondataloven, offentlighedsloven og forvaltningsloven. Som en konsekvens af, at persondataloven ikke gælder for Center for Cybersikkerhed, udstedte Forsvarsministeriet den 13. maj 2013 retningslinier for behandling af personoplysninger m.v. i Center for Cybersikkerhed. Desuden er nogle principper fra persondataloven indskrevet i forslag til lov om Center for Cybersikkerhed.

Med lovforslagets § 8 videreføres undtagelsen af Center for Cybersikkerheds og dermed også GovCERTs virksomhed fra offentlighedsloven, forvaltningsloven og persondataloven. Endvidere udvides GovCERTs grundlag for dataindsamling, da kredsen af virksomheder, der kan tilslutte sig GovCERT, udvides fra virksomheder, der er beskæftiget med kritisk infrastruktur, til en bredere gruppe af virksomheder beskæftiget med samfundsvigtige funktioner. Samfundsvigtige funktioner beskrives i bemærkningerne til lovforslaget som funktioner, der er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed; energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet.

Det fremgår af lovforslaget, at begrundelsen for at placere Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste var at opnå synergieffekter. Institut for Menneskerettigheder finder det imidlertid betænkeligt, at den organisatoriske placering af GovCERT medfører, at GovCERT ikke er omfattet af særligt persondataloven og dermed heller ikke Datatilsynets tilsynsvirksomhed. Evalueringen af GovCERT-loven fremhæver ikke et behov for at fritage GovCERT fra persondataloven, som er af stor betydning i forhold til at sikre en forsvarlig behandling af personoplysninger. Endvidere bemærker instituttet, at der generelt ikke var behov for at undtage GovCERT fra offentlighedsloven, persondataloven og forvaltningsloven, da GovCERT organisatorisk var underlagt IT- og Telestyrelsen.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at GovCERT omfattes

af persondataloven, offentlighedsloven og forvaltningsloven, for eksempel gennem en ændret organisatorisk placering af GovCERT.

3. INTERN VIDEREGIVELSE AF DATA

GovCERT-lovens § 6 regulerede videregivelse af pakkedata fra GovCERT til MILCERT under Forsvarets Efterretningstjeneste. Videregivelse af pakkedata knyttet til en sikkerhedshændelse forudsatte, at IT- og Telestyrelsen skønnede det nødvendigt for at beskytte nationale digitale infrastrukturer mod sikkerhedsmæssige trusler.
Placeringen af både MILCERT og GovCERT i Center for Cybersikkerhed under Forsvarets Efterretningstjeneste medfører, at der nu som udgangspunkt er fri adgang til at udveksle data mellem GovCERT og den øvrige del af Forsvarets Efterretningstjeneste, jf. almindelige forvaltningsretlige principper. Det fremgår af lovforslaget, at Forsvarsministeriet har til hensigt at udstede administrative retningslinier, der sikrer, at intern udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige Efterretningstjeneste sker med respekt for retssikkerheden og den personlige frihed.

Institut for Menneskerettigheder finder det betænkeligt, at der med lovforslaget ikke på lovniveau sikres en varetagelse af retssikkerhedsmæssige hensyn ved videregivelse af oplysninger fra GovCERT til Forsvarets Efterretningstjeneste. Data, som GovCERT er i besiddelse af som den statslige varslingstjeneste for danske myndigheder og en lang række private virksomheder, vil således i høj grad kunne inddrages i Forsvarets Efterretningstjenestes øvrige arbejde inden for det militære område.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at der i lovforslaget indføres et krav om, at videregivelse af data fra GovCERT til resten af Forsvarets Efterretningstjeneste forudsætter, at det konkret vurderes nødvendigt for at beskytte den nationale digitale infrastrukturer mod sikkerhedsmæssige trusler.

4. EKSTERN VIDEREGIVELSE AF DATA

Lovforslagets § 16 regulerer Center for Cybersikkerheds mulighed for ekstern videregivelse af data. Ved begrundet mistanke om en sikkerhedshændelse kan både pakke- og trafikdata videregives til politiet. Trafikdata kan desuden videregives til blandt andet danske myndigheder og udenlandske netsikkerhedstjenester, hvis det vurderes nødvendigt for udførelsen af netsikkerhedstjenestens opgaver.

Det fremhæves i lovforslaget, at en af Center for Cybersikkerheds vigtigste forebyggende aktiviteter er udsendelse af

sikkerhedsvarslinger, hvor myndigheder, virksomheder, andre netsikkerhedstjenester m.v. underrettes om særligt alvorlige sikkerhedshændelser. Det fremhæves endvidere, at et effektivt internationalt samarbejde forudsætter, at Danmark også kan give oplysninger, som kan bidrage til at stoppe grænseoverskridende cyberangreb.

Institut for Menneskerettigheder anerkender behovet for at videregive oplysninger til blandt andet udenlandske netsikkerhedstjenester. Instituttet finder imidlertid også, at muligheden for at videregive oplysninger bør begrænses mest muligt. Instituttet bemærker i den forbindelse at lovforslaget primært fremhæver behovet for at videregive oplysninger vedrørende sikkerhedshændelser. Instituttet finder således, at det bør overvejes, om muligheden for videregivelse af oplysninger bør begrænses yderligere.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at det overvejes at begrænse muligheden for videregivelse af oplysninger i lovforslagets § 16, nr. 2 til trafikdata, der vedrører en konkret sikkerhedshændelse.

5. SLETTEFRISTER

Med lovforslaget udvides fristerne for sletning af data, som ikke knytter sig til en sikkerhedshændelse. Ifølge den nuværende GovCERT-lov kan pakkedata, som ikke knytter sig til en sikkerhedshændelse opbevares i højst 14 dage. Trafikdata, der ikke knytter sig til en sikkerhedshændelse, kan opbevares i højst 12 måneder. I evalueringen af GovCERT-loven fremhæves generelt et behov for længere frister for opbevaring af data. Ifølge lovforslagets § 17, stk. 2, nr. 2, behandles trafik- og pakkedata nu ens, og det foreslås, at opbevaring af sådanne data udvides til højst 13 måneder.

Instituttet finder, at særligt udvidelsen af muligheden for at opbevare pakkedata, som ikke knytter sig til en sikkerhedshændelse, fra 14 dage til 13 måneder er en betydelig udvidelse af adgangen til at opbevare historiske data. Af hensyn til den enkeltes ret til privatliv finder instituttet, at fristerne for sletning af data bør sikre, at oplysninger ikke opbevares længere end højst nødvendigt. Samtidig bør oplysninger kunne opbevares længe nok til, at opgaverne forbundet med GovCERT kan varetages forsvarligt. Instituttet finder det ikke sandsynliggjort i lovforslaget, at en så betydelig udvidelse af adgangen til at opbevare historiske data er et nødvendigt og proportionalt indgreb i den enkeltes ret til privatliv.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at lovforslagets slettefrist på 13 måneder for pakkedata, som ikke knytter sig til en sikkerhedshændelse, sænkes.

Det fremgår desuden af lovforslagets § 17, stk. 4, at data, som er videregivet i medfør af § 16 ikke er omfattet af slettefristerne. I lovforslaget pålægges Center for Cybersikkerhed heller ikke at stille krav om sletning af data hos myndigheder m.v., som modtager data iht. lovforslagets § 16. Ved videregivelse af data, heriblandt til udenlandske myndigheder, er hverken Center for Cybersikkerhed eller modtageren således ifølge lovforslaget forpligtet til at slette de pågældende data.

Det fremhæves i lovforslaget, at Center for Cybersikkerhed i sagens natur ikke har mulighed for at sikre, at der efterfølgende sker sletning af data hos en modtager af disse data. Ved videregivelse af oplysninger til politiet til brug for en eventuel straffesag anses det endvidere for uhensigtsmæssigt, at sådanne oplysninger risikerer at blive slettet af Center for Cybersikkerhed, inden en sådan sag er afsluttet. Det fremhæves desuden i lovforslagets bemærkninger, at danske myndigheder og virksomheder, som modtager data fra Center for Cybersikkerhed vil være underlagt persondatalovens databehandlingsregler.

Institut for Menneskerettigheder finder det ikke tilstrækkeligt godtgjort i lovforslaget, at videregivelse af data ikke kan ske med betingelse om sletning af disse data efter en nærmere angivet periode. Såfremt data videregives til dansk politi til brug for en eventuel straffesag, finder instituttet endvidere, at sletning bør kunne ske, når politiets behandling af sagen er afsluttet.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at der i lovforslagets § 17 indføres krav om sletning af data, som videregives til politiet iht. lovforslagets § 16, nr. 1, når formålet med videregivelsen er ophørt.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at Center for Cybersikkerhed pålægges at indføre krav om sletning af data, som videregives iht. lovforslagets § 16, nr. 2.

6. TILSYNET MED GOVCERT

GovCERTs organisatoriske placering under Center for Cybersikkerhed medfører, at GovCERT er undtaget fra Datatilsynets tilsynsvirksomhed. I den nuværende GovCERT-lov er der etableret et GovCERT-tilsyn. Med

lovforslaget overføres tilsynet med GovCERT imidlertid til Tilsynet med Efterretningstjenesterne, som blev oprettet 1. januar 2014.

Institut for Menneskerettigheder finder som tidligere anført, at GovCERT bør være underlagt persondataloven og herunder tilsyn fra Datatilsynets vedrørende deres behandling af personoplysninger. Såfremt det nuværende forslag opretholdes, hvorefter tilsynet med GovCERT overgår til Tilsynet med Efterretningstjenesterne, bør det sikres, at kompetencen i dette nye tilsyn afspejler den nye opgavevaretagelse.

Det nuværende GovCERT-tilsyn består af en formand, der er jurist og fire sagkyndige medlemmer, der repræsenterer juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab. Det fremgår ikke af lovforslagets bemærkninger, om denne sagkundskab sikres i Tilsynet med Efterretningstjenesterne.

Ved overførslen af tilsynsopgaven fra GovCERT-tilsynet til Tilsynet med Efterretningstjenesterne finder instituttet, at det bør sikres, at en sagkundskab svarende til GovCERT-tilsynets er repræsenteret i Tilsynet med Efterretningstjenesterne.

- Institut for Menneskerettigheder anbefaler – med henblik på at fremme den enkeltes menneskerettigheder – at det sikres, at Tilsynet med Efterretningstjenesterne besidder de fornødne juridiske, it-revisionsmæssige og sikkerhedsmæssige sagkundskab til at foretage et effektivt tilsyn med GovCERT.

Der henvises til sagsnr. 2013/003214.

Venlig hilsen

Rikke Frank Jørgensen og Martin Futtrup

IT-Branchen

04.03.2014

IT-Branchens høringssvar vedr. Lov om Center for Cybersikkerhed

ITB takker for modtaget høring om Lov Center for cybersikkerhed samt evalueringen af GovCert.

Til evalueringen har IT-Branchen følgende kommentar: *"Evalueringen bekræfter, at CFCS udøver et vigtigt og nødvendigt arbejde. Indsatsen har gavnet særligt den offentlige sektors it-sikkerhed i Danmark, og bør fortsættes fremover".*

Generel opbakning
IT-Branchen bakker op om lovforslaget, med nedenstående ændringsforslag og kommentarer.

CFCS fortsat ingen rolle i forhold til overvågning og sikkerhed hos alm. virksomheder
IT-Branchen kan konstatere at lovforslaget lægger op til at CFCS afgrænses klart til at arbejde for offentlige myndigheder og for særligt udvalgte virksomheder der arbejder med samfundsvigtig infrastruktur.

ITB bemærker at der derved fortsat ikke er en CERT eller anden it-sikkerheds-understøttende offentlig instans, der overvåger og kommunikerer om it-sikkerhed hos alm. private virksomheder – de virksomheder der ikke arbejder med samfundsvigtige funktioner.

Afgrænsning ok, hvis andre initiativer støtter op om sikkerhed hos alm. virksomheder
IT-Branchen finder CFCS afgrænsningen i forhold til alm. virksomheder fornuftig, hvis de alm. private virksomheder ved andre snart kommende regeringsinitiativer støttes i retning af en styrket it-sikkerheds-indsats.

- Vi opfordrer konkret regeringen til at prioritere initiativer der styrker alm. virksomheders it-sikkerhed i forbindelse med den kommende vækstplan, der samler op på IKT-vækstteamets anbefalinger om bl.a. it-sikkerhed.

Opgavefordeling og udkonkurrerende virksomhed
IT-Branchen konstaterer der er sket en udvidelse af hvilke virksomheder CFCS kan betjene således at det ikke blot er virksomheder der arbejder med kritisk infrastruktur, men den noget bredere kreds, der arbejder med samfundsvigtige opgaver. Udvidelsen er på den ene side fornuftigt, i forhold til at den hidtidige definition blev oplevet som værende for snæver, så den hæmmede CFCS i at udføre sin opgave. Men udvidelsen kan være problematisk og virke udkonkurrerende for private it-sikkerhedsleverandører, hvis ikke der gøres særlige anstrengelser for at sikre, at CFCS supplerer og samarbejder med, frem for at udkonkurrere private it-sikkerheds-aktører.

IT-Branchen opfordrer derfor til, at det tydeliggøres i lovforslaget,

- "at CFCSs virke i videst muligt udstrækning skal virke supplerende fremfor konkurrerende for den indsats private it-sikkerhedsleverandører udfører
- "at CFCS i udgangspunktet ikke selv bør udføre opgaver, installere udstyr eller sælge serviceydelser, som private it-sikkerhedsleverandører kunne have løst eller installeret. På særligt udvalgte områder der er undtagelsen herfra, skal CFCS tilstræbe at konkurrence-udbyde opgaven til varetagelse af en eller flere private leverandører for en tidsafgrænset periode.

Vidensdeling med sikkerhedsleverandører bør eksplicit fremgå som en prioriteret opgave
IT-Branchen konstaterer at det i dag er et problem for forebyggelsen af angreb på tværs af virksomheder og myndigheder, at viden ikke deles systematisk i Danmark.

Der opleves en uheldig tendens til at viden der opstår i den private sektor forbliver hos den enkelte virksomhed, fordi enhver kommunikation herom udadtil betragtes som risikofyldt, for eks. omdømme og kundeloyalitet. Og at viden som opstår hos offentlige myndigheder for ofte og ukritisk hemmelighedstemples med argumentet om at skulle værne om den enkelte myndigheds eller kritisk infrastrukturs sikkerhed, eller for at værne om aktuel efterforskning.

Resultatet er at forsvaret mod cyberangreb sjældent bliver proaktivt baseret på nyeste fælles viden i offentlig og privat sektor. Forsvaret bliver mere reaktivt og baseret på det mere afgrænsede indblik som er lokalt tilstedet i den enhed, sektor eller branche man er en del af og hos den konkrete evt. sikkerheds-leverandør, man rådgiver sig hos. En leverandør, der vel og mærke også kan opleve udfordringer med at samle viden bredt om angrebsmønste etc.

IT-Branchen anser Lov om Center for Cybersikkerhed som én blandt flere mulige anledninger til at få igangsat et skift imod en mere konstruktivt vidensdelende indsats. IT-Branchen foreslå derfor, at lovforslaget suppleres med bestemmelser der forpligter CFCS til at deltage aktivt vidensdelende med omverdenen. Eks. med supplerende lovformuleringer som

- *"At Center for Cybersikkerhed skal samarbejde vidensdelende med private it-sikkerheds-leverandører, og løbende via disses danske brancheorganisationer dele aggregeret anonymiseret data om hvilke angreb og trusler der kan konstateres hos de tilknyttede myndigheder og virksomheder."*

IT-Branchen bemærker at den viden der foreslås delt *ikke omfatter* henførbart navn på virksomheder, myndigheder eller personer der er blevet ramt, ej heller konkret pakkedata med eks. indhold, som måtte være blevet registeret i behandlingen af en sikkerhedshændelse. Men derimod aggregeret data om hvilke trusler der ses mod hvilke typer af systemer, hvilke angrebsmetoder der anvendes og hvilke modforanstaltninger der ses værende effektfulde til bekæmpelse heraf.

Denne vidensdeling skal ske i respekt for de i loven nævnte fortrolighedshensyn, samt beskyttelsen af nationale interesser. Men det er vigtigt, at CFCS ikke gives for let adgang til at undtage viden for vidensdelingen med henvisning hertil. Et mere sammenhængende effektivt forsvar kræver af viden deles i højere grad end nu. Uden udadvendt vidensdeling ses CFCS ikke anvendt optimalt i forhold til styrkelsen af et proaktivt informationssikkerhedsniveau i Danmark.

Begræns masseindsamlingen, men gem data i længere tid for midlertidigt tilsluttede virksomheder med begrundet mistanke om angreb

IT-Branchen anser generelt set telelogningsreglerne for overdrevne og unødigt fordyrende for virksomheder. Vi skal som samfund være påpasselige med, hvilken masseindsamling af data vi igangsætter, ikke mindst, hvis de indsamlede data kun meget sjældent anvendes. IT-Branchen ønsker derfor telelogningsreglerne afskaffet, til fordel for en ny model hvor udbydere på baggrund af domstolskendelser eller specifikt begrundende anmodninger hos myndigheders sikkerhedstjenester kan blive pålagt at iværksætte konkret logning af personer eller juridiske enheder, der er under begrundet mistanke for eks. terror eller anden alvorlig kriminalitet. Centralt er at virksomheder kompenseres for udgiften til denne logning og holdes ansvarsfri for evt. følgevirkninger af eks. at skulle blokere for tjenester eller trafik i en periode.

Derfor anser vi det i udgangspunktet for værende positivt, at der i lovforslag om Center for Cybersikkerhed angives klare regler for dataindsamlingens formål, tidsgrænser for opbevaring og for sletning af indsamlede data og metadata. Vi fraråder dog jf. argumenterne ovenfor at tidsgrænsen for den generelle dataindsamling forlænges til 13 måneder for så vidt angår data, der ikke er begrundet mistanke om er af betydning for konkrete it-sikkerheds-angreb.

Omkring virksomheder eller myndigheder der midlertidigt tilsluttes som følge af konkrete hændelser og begrundet mistanke om sikkerheds-hændelser kan der dog være behov for at opsamle og opbevare data i længere perioder end foreslået i lovforslaget. Dette som følge af at der i mange tilfælde går lang tid, typisk 8-9 måneder, før du opdager det fulde omfang af, hvordan din sikkerhed er blevet kompromitteret.

Dette sker bl.a. som følge af, at it-kriminelle er begyndt at bruge samtidige kombinationer af meget åbenlyse angreb og mere svært identificerbare angreb mod samme mål. Det der umiddelbart ligner eks. et DDOS-angreb kan være et røgslør for et andet samtidigt angreb, der ændrer i eller udtrække følsomme data fra kernesystemer.

I lyset af den erfaring og udvikling, anbefaler IT-Branchen, at

- lovforslagets frist for den midlertidige tilslutning af virksomheder forlænges fra nuværende periode på 2 måneder, til en periode på "op til 12 måneder".
- at tidsfristen for hvor længe data skal opbevares hvis den ikke er knyttet til en konkret og begrundet mistænkelig sikkerhedstrussel, tilbageføres til det hidtidige niveau, der kendes fra lov om GovCert.

Vi vurderer at dét setup fornuftigt afvejer ulemperne ved dataindsamlingen med formålet om at styrke overblikket over og bekæmpelsen af cyberkriminalitet.

Tilslut kun virksomheder midlertidigt når alle forudsætninger er opfyldt

IT-Branchen gør opmærksom på, at lovforslaget bør tydeliggøres omkring § 6, som omhandler indgreb i meddelelseshemmeligheden.

- I bestemmelse 1 bør tilføjes et afsluttende "**, og**", så §6, bestemmelse 1 lyder:
  "... myndigheden eller virksomheden har givet skriftligt samtykke til behandlingen, ***og****"*

Tilføjelsen tydeliggør, at der både kræves 1) samtykke fra virksomheden, og jf. bestemmelse 2 er foretaget et relevans skøn, samt jf. bestemmelse 3) at overvågningen er af midlertidig karakter.

IT-Branchen anser det for værende væsentligt for erhvervslivet såvel som offentlighedens tillid til hvilken funktion CFCS udøver, at der ikke kan opstå misforståelse om, hvorvidt staten uden virksomheders samtykke kan tvangstilslutte dem en overvågning, selvom den blot er midlertidig. Vi ønsker ikke et samfund, hvor virksomheder kan frygte for, at egne statsinstitutioner overvåger dem, uden deres samtykke.

Gennemsigtighed og evaluering
Afslutningsvist foreslår IT-Branchen

- at CFCSs pålægges for offentligheden at aflevere en årlig gennemsigtighedsrapport, der informerer generelt om, i hvilket omfang CFCS i forbindelse med sit virke griber ind i meddelelseshemmeligheden hos tilsluttede myndigheder og virksomheder.
- at det i loven indskrives, at CFCSs virke skal evalueres senest efter 4 år, med fokus på betydning for sikkerheden, for meddelelseshemmeligheden, for det private marked for it-sikkerhed og dets evne til at vidensdele løbende med selvsamme.

IT-Branchen takker for muligheden for at kommentere, og ønsker Center for Cybersikkerhed fortsat god arbejdslyst med sit nødvendige virke.

Med venlig hilsen

Morten Bangsgaard
IT-Branchen

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt pr email til: fmn@fmn.dk
med kopi til: pah@fmn.dk og hvs@govcert.dk

IT-Politisk Forening
c/o Niels Elgaard Larsen
Århusgade 35, 1.
2100 København Ø

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 2014-03-04

Høringssvar om udkast til forslag til Lov om Center for Cybersikkerhed

Udkast til lovforslag om Center for Cybersikkerhed (fremover: lovforslaget) er en videreførelse af den eksisterende GovCERT-lov med en række tilpasninger. Nogle af disse tilpasninger skyldes flytningen af området til Forsvarets Efterretningstjeneste, mens andre er udtryk for et ønske om flere beføjelser til det nye Center for Cybersikkerhed.

IT-Politisk Forening mener at IT-sikkerhed (cybersikkerhed) er en væsentlig samfundsmæssig opgave, og det er uden tvivl hensigtsmæssigt at samle ansvaret for cybersikkerheden på statens område i en enkelt enhed.

Men vi er samtidig stærkt bekymret for de beføjelser til indgreb i meddelelseshemmeligheden uden dommerkendelse, som Center for Cybersikkerhed får med dette lovforslag. På en række punkter mener vi at beføjelserne er for vidtgående.

Behov for præcisering af om en internetudbyder kan tilslutte sig netsikkerhedstjenesten

Det fremgår af bemærkningerne til lovforslaget, at det først og fremmest er statslige myndigheder som kan tilsluttes GovCERT, men samtidig lægges der op til en udvidelse af kredsen af offentlige myndigheder og private virksomheder som kan tilsluttes den nye netsikkerhedstjeneste.

En større dansk internetudbyder må siges at udgøre en

samfundsvigtig funktion, og en internetudbyder kan muligvis tilslutte sig allerede under den gældende GovCERT-lov. Det fremgår i øvrigt af evalueringen af GovCERT-loven, at virksomheden TDC er tilsluttet, men det fremgår ikke hvilke funktioner hos TDC som er tilsluttet (specielt: er det TDC som internetudbyder der er tilsluttet?).

I den forbindelse vil IT-Politisk Forening påpege, at rækkevidden af indgrebet i meddelelseshemmeligheden (lovforslagets kapitel 4) er meget større, hvis indgrebet er rettet mod en internetudbyder.

Hvis en statslig myndighed er tilsluttet ordningen, får netsikkerhedstjenesten kun adgang til de oplysninger, som borgerne selv giver til denne myndighed. Hvis der derimod er adgang til at indsamle pakkedata fra en internetudbyder for at beskytte den danske internet-infrastruktur, vil staten få en generel adgang til borgernes private kommunikation via internettet, herunder eksempelvis fortrolig kommunikation med journalister og advokater.

En vurdering af nødvendighed og proportionalitet i forhold til EMRK artikel 8, som er foretaget med udgangspunkt i at en statslig myndighed tilslutter sig, kan efter vores opfattelse slet ikke overføres til den situation, hvor en internetudbyder tilslutter sig. Det samme gælder en indholdstjeneste med et stort antal brugere, for eksempel et socialt medie som Facebook.

I forbindelse med høringen om GovCERT-loven (lovforslag L 197, 1. samling 2010-11) skrev IT-Politisk Forening følgende i vores høringssvar:

> *Den statslige varslingstjeneste bør ikke være bemyndiget til at opsamle eller tilgå datatrafik, hvor hverken afsender eller modtager frivilligt og eksplicit har tilsluttet sig tjenesten.*
>
> *Selvom det ikke er GovCERT's nuværende sigte, finder IT-Politisk Forening det vigtigt, at danske internetbrugere ikke kan blive overvåget af en statslig tjeneste, selvom internetudbydere skulle tilslutte sig varslingstjenesten.*

Denne bemærkning blev citeret i høringsnotatet ved

fremsættelse af GovCERT-loven i 2011, men det blev desværre ikke præciseret i høringsnotatet, om det skulle være muligt for en internetudbyder at tilslutte sig varslingstjenesten.

IT-Politisk Forening vil opfordre til, at Folketingets partier eksplicit tager stilling til dette væsentlige spørgsmål i forbindelse med behandlingen af lovforslaget.

Det er fortsat vores opfattelse, at der kun bør registreres trafik- og pakkedata, hvis afsender eller modtager eksplicit er tilsluttet netsikkerhedstjenesten. Internettrafik, som en internetudbyder alene videreformidler fra afsender til modtager som transittrafik, bør ikke overvåges og registreres af staten på denne måde.

Udvidelse af kredsen af private virksomheder som kan tilslutte sig

Bemærkningerne til lovforslaget lægger op til at udvide (især) kredsen af private virksomheder, som kan tilsluttes netsikkerhedstjenesten. Det er ikke længere et krav, at der er tale om virksomheder som beskæftiger sig med kritisk infrastruktur. Alle virksomheder, som kan blive udsat for et cyberangreb, kan efter § 6 og § 7 blive tilsluttet på midlertidig basis.

IT-Politisk Forening mener ikke, at der er et reelt behov for denne udvidelse af kredsen af virksomheder, som kan tilslutte sig netsikkerhedstjenesten. Center for Cybersikkerhed bør koncentrere sig om statslige og andre offentlige myndigheder, samt enkelte private virksomheder som udfører samfundskritiske opgaver (dog ikke internetudbydere).

For det første ønsker vi at begrænse indgrebet i meddelelseshemmeligheden, og det bør være forudsigeligt for borgerne hvornår trafik- og pakkedata videregives til den statslige netsikkerhedstjeneste. For det andet mener vi, at private virksomheder selv kan varetage deres IT-sikkerhed, og det er ikke hensigtsmæssigt at private sikkerhedsfirmaer skal konkurrence med en statslig netsikkerhedstjeneste, som via særlovgivning har fået beføjelser som de private firmaer ikke har.

Betingelsen for at inddrage private virksomheder efter § 6 og § 7 og foretage indgreb i meddelelseshemmeligheden er at der er en begrundet mistanke om en sikkerheds-hændelse. Men cyberangreb er ofte kortvarige, så det krav virker ikke særligt operationelt og beskyttende for borgernes ret til privatliv. Indgrebet i meddelelses-hemmeligheden sker allerede når den private virksomhed midlertidigt tilslutter sig den statslig netsikkerheds-tjeneste, og der sker registrering af trafik- og pakkedata hos den statslige tjeneste.

Definition at trafikdata

Klassificering som trafikdata eller pakkedata har betydning for hvem oplysningerne kan videregives til. I den eksisterende GovCERT-lov har det desuden betydning for hvor længe oplysningerne kan opbevares, men den forskel er ikke videreført i det nye lovforslag, jf. nedenfor.

Trafikdata defineres i lovforslaget som

> *Ved trafikdata forstås data, som behandles med henblik på overførsel af pakkedata. Det vil sige data, som beskriver oprindelse, destination og rutestyringsinformation, herunder oprindelses-domænet eller den oprindelige elektroniske adresse samt anden tilsvarende information. Trafikdata kan eksempelvis være header-informationen i digitale kommunikationsprotokoller, men vil også omfatte protokoller, der udelukkende anvendes til rute- og kommunikationsstyring, f.eks. DNS og SIP. Konkrete eksempler på trafikdata er oplysninger om IP-adresser, e-mailadresser, hjemmesideadresser, browserversioner, kommunikationens varighed og tidspunktet for kommunikationen.*

Denne definition er bredere end definitionen af trafikdata i e-privacy direktivet 2002/58/EF. Her er trafikdata alene data som er nødvendig for overførsel af kommunikation i et elektronisk kommunikationsnet. Hvis der eksempelvis er tale om en forespørgsel til en webserver, er domæne-navnet, IP adressen og portnummeret nødvendige for at overføre data til webserveren, mens URL-oplysninger om den specifikke hjemmesideadresse alene behandles af webserveren, og derfor ikke kan betegnes som trafikdata i

forhold til e-privacy direktivet. Oplysninger om browser-versioner kan heller ikke med rimelighed betragtes som trafikdata.

IT-Politisk Forening mener, at trafikdata skal defineres mere snævert i overensstemmelse med e-privacy direktivet 2002/58/EF.

Udvidelse af opbevaringsperioden for trafikdata og pakkedata

Med lovforslaget foreslås en kraftig udvidelse af den periode, hvor trafikdata og pakkedata kan opbevares. Data der knytter sig til en sikkerhedshændelse kan fortsat opbevares i tre år.

For trafikdata udvides opbevaringsperioden fra 12 måneder til 13 måneder, mens lovforslaget for pakkedata udvider perioden fra 14 dage til 13 måneder. Lovforslaget opererer altså med en fælles opbevaringsperiode for begge typer data.

Forsvarsministeriets begrundelse for denne udvidelse er muligheden for at tegne et normalbillede af internetaktiviteterne hos den enkelte myndighed, så netsikkerhedstjenesten bedre kan opdage en sikkerhedshændelse. Hvis der hos en myndighed eksempelvis gennemføres en ekstern backup en gang om måneden, vil det generere et atypisk trafikmønster. En anden begrundelse er muligheden for at spore cyberangreb, som ikke tidligere er opdaget.

For så vidt angår muligheden for at tegne et normalbillede af aktiviteten, har IT-Politisk Forening meget vanskeligt ved at se behovet for at gemme pakkedata i 13 måneder. Myndighederne bør være klar over hvornår der foretages backup, så denne trafik eventuelt helt kan undtages. Under alle omstændigheder må aggregerede statistikker for ind- og udgående trafikmængder være tilstrækkelige til at tegne et normalbillede. Det er slet ikke nødvendigt med hverken trafik- eller pakkedata her.

Selvfølgelig er der altid en teoretisk mulighed for at nye oplysninger gør det muligt at opdage cyberangreb, som tidligere blev overset, men IT-Politisk Forening synes ikke

at der er den fornødne proportionalitet i forhold til at pakkedata (indholdsdata) kan opbevares i op til 13 måneder. Lovforslaget siger samtidig at 13 måneder er den maksimale opbevaringsperiode, og at data skal slettes når formålet med behandlingen er opfyldt. Men hvis et af formålene er at kunne opdage sikkerhedshændelser tilbage i tid, bliver data aldrig slettet før udløbet af fristen på 13 måneder.

IT-Politisk Forening mener, at de eksisterende opbevaringsfrister skal bevares, og i særdeleshed at pakkedata kun skal opbevares kortvarigt.

Behandling af krypterede pakkedata

Efter den nuværende GovCERT-lov sker der ikke nogen behandling af krypterede pakkedata eller forsøg på at de-kryptere disse. Denne begrænsning forslås ikke videreført.

IT-Politisk Forening skal bemærke, at det i praksis vil medføre et krav om at den statslige netsikkerhedstjeneste får adgang til private krypteringsnøgler for de tilsluttede myndigheder og virksomheder. Hvis HTTPS trafik skal overvåges af monitoreringsudstyr før webserveren, skal dette udstyr reelt foretage et (kontrolleret) man-in-the-middle angreb på trafikken.

Problemet med den type indgreb i end-to-end krypteringen mellem afsender og modtager er at man risikerer, at der skabes nye sikkerhedshuller som kan udnyttes af andre. I det konkrete tilfælde kan en overvågningsmulighed for krypteret webtrafik (HTTPS) indebære en risiko for at en ekstern angriber (for eksempel "cyberkriminelle") også får mulighed for at skaffe sig adgang til trafikken, og derved kompromittere personlige oplysninger for danske borgere.

Denne risiko bør nøje overvejes inden initiativer mod krypteret trafik igangsættes. Det bør præciseres i bemærkningerne til lovforslaget, at analyse af krypterede pakkedata ikke under nogen omstændigheder må medføre nye sikkerhedsrisici for borgerne.

Indarbejdelse af borgerbeskyttelse fra persondataloven

Forsvarets Efterretningstjeneste er ikke omfattet af persondataloven, men lovforslagets kapitel 6 indeholder en beskyttelse der formelt svarer til persondatalovens regler om behandling af personoplysninger. Denne beskyttelse er dog ikke reel, da netsikkerhedstjenesten primært behandler personoplysninger fra indgrebet i meddelelseshemmeligheden efter kapitel 4, og disse oplysninger er eksplicit undtaget fra beskyttelsen i §§ 10-12.

Oplysninger om hvilke myndigheder og virksomheder der er tilsluttet

GovCERT har i forbindelse med evalueringen af GovCERT-loven offentliggjort en liste med de myndigheder og virksomheder som er tilsluttet den eksisterende varslingstjeneste.

Det er ikke klart for IT-Politisk Forening, om disse oplysninger fortsat vil være tilgængelige for offentligheden? Det fremgår nemlig af lovforslaget, at Center for Cybersikkerhed er undtaget fra offentlighedsloven.

IT-Politisk Forening mener, at det er særdeles vigtigt, at borgerne altid kan få oplyst hvornår deres trafik- og pakkedata risikerer at blive registreret af Forsvarets Efterretningstjeneste.

På trods af den generelle undtagelse fra offentlighedsloven, bør Center for Cybersikkerhed være forpligtet til løbende at offentliggøre hvilke myndigheder og virksomheder der er tilsluttet ordningen. Det bør også gælde for virksomheder, som er midlertidigt tilsluttet efter § 6 og § 7.

Tilsynet med behandlingen af personoplysninger

Efter den nuværende GovCERT-lov skal der være et uafhængigt tilsyn med GovCERT, som desværre først er oprettet i september 2013, mere end to år efter GovCERT-

lovens ikrafttræden. Forsvarsministeriet vil med lovforslaget overdrage denne opgave til Tilsynet med Efterretningstjenesterne.

Forsvarsministeriet bemærker selv, at tilsynet med Center for Cybersikkerhed vil adskille sig fra de tilsynsopgaver, som allerede udføres af Tilsynet med Efterretningstjenesterne.

I den forbindelse skal man være opmærksom på at PET's beføjelser i forhold til borgerne generelt er reguleret af retsplejeloven med domstolskontrol, og at FE's aktiviteter primært er rettet mod udlandet og ikke direkte mod danske borgere (medmindre forsvarslovens § 17 er i anvendelse). Center for Cybersikkerhed får derimod beføjelser til at foretage indgreb i meddelelses-hemmeligheden i forhold til danske borgere uden nogen domstolskontrol.

Udover det ret vidtgående indgreb i meddelelses-hemmeligheden, skal tilsynet med Center for Cybersikkerhed kontrollere, at de indsamlede oplysninger kun anvendes til formål der vedrører cybersikkerhed, og ikke inddrages i FE's almindelige arbejde, jf. afsnit 3.5.3 i lovforslagets bemærkninger.

IT-Politisk anbefaler, at det nøje overvejes, om Tilsynet med Efterretningstjenesterne har de kompetencer, som er nødvendige for at føre et effektivt tilsyn med Center for Cybersikkerhed. Den nuværende GovCERT-lov anfører i § 7, stk. 2 de kompetencer som skal være til stede i det eksisterende tilsyn.

Foruden de kompetencer som er nævnt i § 7, stk. 2 i GovCERT-loven, bør Tilsynet også foretage en vurdering af konsekvenserne for borgernes ret til privatliv, herunder en løbende vurdering af nødvendighed og proportionalitet i forhold til EMRK artikel 8.

Årlig redegørelse fra Tilsynet

Efter lovforslagets § 24 skal Tilsynet udgive en årlig redegørelse, som skal offentliggøres. IT-Politisk Forening mener, at det er vigtigt at denne redegørelse indeholder aggregerede oplysninger, som giver Folketinget og

borgerne mulighed for at vurdere omfanget af indgrebet i meddelelseshemmeligheden samt omfanget af videregivelse af oplysninger efter kapitel 7.

Det kunne for eksempel være en skønsmæssig vurdering af hvor mange danske IP adresser ("borgere") der er berørt af henholdsvis indgrebet i meddelelseshemmeligheden og videregivelse af oplysninger til eksterne samarbejdspartnere i ind- og udland.

Som anført ovenfor bør det også fremgå hvem der er tilsluttet den statslige netsikkerhedstjeneste.

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt pr email til: fmn@fmn.dk
med kopi til: pah@fmn.dk og hvs@govcert.dk

IT-Politisk Forening
c/o Niels Elgaard Larsen
Århusgade 35, 1.
2100 København Ø

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 2014-03-04

Høringssvar om udkast til evaluering af GovCERT-loven

IT-Politisk Forening har følgende korte bemærkninger til evalueringen af GovCERT-loven.

Tilsynet med GovCERT

Det er beklageligt at tilsynet med GovCERT, jf. lovens § 7, først blev nedsat i september 2013, og at der derfor ikke foreligger en årsrapport fra tilsynet. Det kunne have været væsentlig information i forhold til at vurdere de opgaver, som tilsynet med Center for Cybersikkerhed skal varetage, herunder hvilke faglige kompetencer (sagkundskab) som tilsynet bør besidde.

Bidrag til cybersikkerheden

Under punktet GovCERT's konkrete bidrag til cybersikkerheden nævnes kompromitteringen af Erhvervs- og Vækstministeriets systemer samt den meget omtalte hackersag hos CSC.

IT-Politisk Forening undrer sig over at CSC nævnes i den forbindelse, da CSC ikke er tilsluttet GovCERT, og kompromitteringen af CSC's systemer blev først opdaget, da svenske myndigheder gjorde de danske myndigheder opmærksom på at der var sket indtrængen i CSC's systemer.

I begge sager har GovCERT givetvis ydet væsentlige bidrag til opklaring af hvad der er sket, men hovedformålet med IT-sikkerhed, hvad enten det er i statsligt eller privat regi, er at stoppe uautoriseret indtrængen og

kompromittering af data. Desværre kan det ikke ud fra evalueringen vurderes i hvilket omfang GovCERT har bidraget til dette.

Konsekvenserne for borgernes ret til privatliv

Evalueringen omfatter desværre ikke GovCERT's konsekvenser for borgernes ret til privatliv. IT-Politisk Forening vil opfordre til at evalueringsrapporten udvides med et afsnit om dette inden lovforslaget om Center for Cybersikkerhed fremsættes i Folketinget.

GovCERT's funktionen indebærer et indgreb i meddelelseshemmeligheden uden krav om mistanke eller nogen form for domstolskontrol. Det giver anledning til væsentlige betænkeligheder i forhold til bl.a. EMRK artikel 8.

Retten til privatliv efter EMRK artikel 8 er ikke absolut, men indskrænkninger af denne ret skal opfylde en række betingelser om især nødvendighed og proportionalitet. Det bør løbende vurderes dels om disse betingelser er opfyldt, dels om en mindre vidtgående indskrænkning kunne være tilstrækkelig i forhold til opfyldelse af formålet om sikring af den danske cybersikkerhed.

Vestre Landsret
Præsidenten

Forsvarsministeriet
Holmens Kanal 42
1060 København K

J.nr. 40A-VL-6-14
Den 03/03-2014

Forsvarsministeriet har ved brev af 4. februar 2014 anmodet om eventuelle bemærkninger til et udkast til forslag til lov om Center for Cybersikkerhed og et udkast til Evaluering af GovCERT-loven.

I den anledning skal jeg meddele, at landsretten ikke finder anledning til at udtale sig om udkastene.

Dette svar sendes efter anmodning pr. e-mail til fmn@fmn.dk med kopi til pah@fmn.dk og hvs@govcert.dk.

Der henvises til sagsnummer 2013/003214.

Med venlig hilsen

Bjarne Christensen

Østre Landsret
Præsidenten

Den 12/02-2014
J.nr. 40A-ØL-9-14
Init:maa

Forsvarsministeriet
Holmens Kanal 42
1060 København K

Sendt pr. mail til fmn@fmn.dk, pah@fmn.dk og hvs@govcert.dk

Justitsministeriet har ved brev af 4. februar 2014 (Sagsnr. 2013/003214) anmodet om eventuelle bemærkninger til forslag til høring over udkast til forslag til lov om Center for Cybersikkerhed samt Evaluering af GovCERT-loven.

I den anledning skal jeg meddele, at udkastet ikke giver landsretten anledning til at fremkomme med bemærkninger.

Med venlig hilsen

Bent Carlsen

RETSPOLITISK FORENING

HØRINGSSVAR

Høring over udkast til forslag til Lov om Center for Cybersikkerhed

Sagsnummer: 2013/003214

Generelle bemærkninger.

Det fremgår af regeringsgrundlaget, at de forskellige myndigheders indsats i beskyttelsen mod cyberangreb mv. samles i et IT sikkerhedscenter (under Forsvarsministeriet), der skal varetage opgaven som den nationale IT-sikkerhedsmyndighed. Dette fremgår tillige af loven om Forsvarets Efterretningstjeneste § 1 stk. 3 hvorefter Forsvarets Efterretningstjeneste er national it-sikkerhedsmyndighed, militær varslingstjeneste for internettrusler m.v. (MILCERT) og statslig varslingstjeneste for internettrusler (GovCERT).
At FE skal varetage civile IT-sikkerhedsopgaver er nyt for Retspolitisk Forening.

Foreningen har ikke haft mulighed for at udtale sig om denne overførsel af civile IT-sikkerhedsopgaver. Foreningen har heller ikke haft mulighed for at udtale sig om lovforslaget om Forsvarets Efterretningstjeneste, da dette så vidt ses ikke blev sendt i høring. Det fremgår af bemærkningerne til lovforslaget om Forsvarets Efterretningstjeneste (L 163 alm. bemærkninger pkt. 3.1.3):

" FEs opgaver som national it-sikkerhedsmyndighed m.v.

Ved den kongelige resolution af 3. oktober 2011 blev »ressortansvaret for sager vedrørende beskyttelse af kritisk it-infrastruktur samt statens varslingstjeneste for internettrusler GovCERT« overført til Forsvarsministeriets område. Endvidere fremgår det af regeringsgrundlaget af samme dato, »Et Danmark, der står sammen«, at »regeringen vil med respekt for retssikkerheden og den personlige kommunikationsteknologi er vigtig for landets økonomi og sikkerhed. For at styrke beskyttelsen mod cyberangreb m.v. samles de forskellige myndigheders indsats i et IT sikkerhedscenter (under Forsvarsministeriet), der skal varetage opgaven som den nationale IT-sikkerhedsmyndighed og Governmental Computer Emergency Response Team (GovCERT).«

Som det fremgår af lovforslagets § 1, stk. 3, har Forsvarets Efterretningstjeneste til opgave at være national it-sikkerhedsmyndighed. Som national it-sikkerhedsmyndighed varetager Forsvarets Efterretningstjeneste bl.a. visse af de opgaver, der er fastlagt i cirkulære nr. 204 af 7. december 2001 vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (det såkaldte sikkerhedscirkulære). Sikkerhedscirkulæret vil blive

tilpasset i overensstemmelse med dette, og det er i den forbindelse hensigten, at det skal fremgå, at funktionen i relation til politiet og anklagemyndigheden fortsat varetages af PET.

Endvidere har FE til opgave at være militær varslingstjeneste for internettrusler m.v. (MILCERT) og statslig varslingstjeneste for internettrusler m.v. (GovCERT).

GovCERT er aktuelt reguleret i lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v.

Forsvarsministeriet har til hensigt at fremsætte forslag til en særskilt lov om Center for Cybersikkerhed. Centerets virksomhed er således ikke nærmere reguleret af dette lovforslag".

Til grund for udvalgsarbejdet i Folketinget blev alene fremsendt høringssvar vedr. betænkning nr. 1529 om PET og FE. Denne betænkning indeholdt hverken i betænkningens tekst eller i sit lovudkast om Forsvarets Efterretningstjeneste nogen bemærkninger endsige vurdering af overførsel af civile IT-sikkerhedsopgaver. Jf. lovudkastets § 2 stk.1. og bemærkningerne hertil (bet. 1529 s. 596).

Foreningen skal udtale sin skarpeste kritik af dette hændelsesforløb. Såfremt L 163 havde været sendt i høring med denne væsentlig ændring, havde de høringsberettigede været i stand til at forholde sig til det ovenfor gengivne afsnit af lovforslagets bemærkninger. Nu er de hørte myndigheder og organisationer bragt i en situation, hvor de principielle overvejelser om FE's civile opgaver ikke kan fremkomme i den relevante sammenhæng, da opgaverne allerede er overført til FE med FE-loven.

Foreningen har herefter følgende bemærkninger til lovudkastet om Center for Cybersikkerhed.

Foreningen finder, at den anførte begrundelse herfor, at :" *... placeringen af Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste var særligt at opnå synergieffekter i form af eksempelvis udnyttelse af Forsvarets Efterretningstjenestes erfaringer inden for it-sikkerhedsområdet, viden om det internationale trusselsbillede på cyberområdet og særlige adgang til oplysninger fra udlandet om cybertrusler* ", ikke forekommer særligt overbevisende, når lovforslaget i alt væsentligt drejer sig om civile sikkerhedsopgaver, jf. forslagets generelle bemærkninger (s.10) hvor det anføres, "*...at Forsvarets Efterretningstjeneste vurderer, at de alvorligste cybertrusler mod Danmark i øjeblikket kommer fra statslige aktører, der udnytter internettet til at spionere og stjæle dansk intellektuel ejendom, f.eks. patenteret viden, forskningsresultater og forretningshemmeligheder. Truslen kommer navnlig fra stater, som bruger informationerne til at understøtte deres egen økonomiske, militære og samfundsmæssige udvikling".*

Disse opgaver kunne uden at antaste udnyttelsen af FE's erfaringer inden for it-sikkerhedsområdet formentlig uden problemer være ført tilbage til et civilt sikkerhedscenter underlagt Datatilsynets kontrol, således som det var tilfældet med GovCERT (Governmental Computer Emergency Response Team.), der tidligere var en del af IT og Telestyrelsen, jf. lov nr.596 af 14. juni 2011. Etablering af et samarbejde med henblik på en udnyttelse af tjenestens erfaringer på området, ville næppe volde større vanskeligheder. Den aktuelle debat om NSA's overvågning af væsentlige samfundsfunktioner i lande uden for USA samt overvågning af privat datatransmission forekommer som et velegnet eksempel på en oplagt samarbejdsmulighed.

Såfremt GovCERT-opgaverne skal forblive under Forsvarets Efterretningstjeneste, finder foreningen, at dette af hensyn til de nedenfor anførte forhold, bør kunne ske i form af en særlig civil IT-sikkerhedsafdeling, der er underlagt persondataloven og tilsyn af Datatilsynet.

Forholdet til persondataloven.
Det hedder videre i bemærkningerne (s.11), at *"Da Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste, finder persondataloven således ikke anvendelse på centerets virksomhed. Med lovforslaget foreslås det imidlertid, at en række af de centrale principper i persondataloven også skal finde anvendelse på Center for Cybersikkerheds virksomhed. Datatilsynet vil dog ikke skulle føre tilsyn med Center for Cybersikkerheds overholdelse af lovforslagets bestemmelser om behandling af personoplysninger. Denne tilsynsopgave vil blive varetaget af Tilsynet med Efterretningstjenesterne"*.

Dette er efter Retspolitisk Forenings opfattelse et helt afgørende problem ved centrets placering. Foreningen finder, at der dermed sker en betænkelig udhuling af persondataloven samtidig med, at der konstrueres en retstilstand, hvor visse centrale principper alligevel skal finde anvendelse. Der institueres så at sige en halv persondatalov for centrets arbejde. Foreningen skal derfor foreslå, at såfremt centret administrativt absolut skal placeres under FE, at problemstillingen vendes om således, at persondataloven er gældende med de modifikationer, som følger af et administrativt fællesskab med en efterretningstjeneste.

Tilsyn.
Det foreslås tillige, at tilsynet med efterretningstjenesterne skal varetage tilsynet med centret. I betragtning af den altovervejende civile karakter af centrets opgaver, jf. ovenfor, forekommer det ikke logisk at placere tilsynsfunktionen hos et organ, der særligt er etableret med henblik på kontrol med en efterretningsvirksomhed for så vidt angår registrering af personoplysninger. Foreningen finder, at de beføjelser, der er tillagt Tilsynet med Efterretningstjenesterne, jf. § 13 i lov om Forsvarets Efterretningstjeneste samt særligt lovens § 10, er så beskedne, at de i praksis næppe har nogen værdi som sikring af enkeltindividers og juridiske personers retssikkerhed. Set i lyset af bestemmelserne i persondatalovens kapitel 9 bliver dette endnu tydeligere.

Foreningen finder derfor, at tilsynet med centrets registrering af personoplysninger bør placeres hos Datatilsynet.

Bestemmelser om sletning af data.
Det fremgår af bemærkningerne (s.24) at:"... *data, der er knyttet til en sikkerhedshændelse, fortsat højst må opbevares tre år, hvorefter de skal slettes. Det er samme tidsmæssige grænse, som er fastsat i GovCERT-lovens § 4, stk. 3.*

For så vidt angår øvrige data, der ikke er knyttet til en sikkerhedshændelse, foreslås det, at der fastsættes en fælles opbevaringsperiode på højst 13 måneder, som giver mulighed for at undersøge, om myndigheder og virksomheder har været udsat for hidtil uopdagede cyberangreb samt foretage år til-år-sammenligninger af normalbilledet hos de tilsluttede myndigheder og virksomheder. Som efter gældende ret vil der være tale om maksimale opbevaringsperioder. Center for Cybersikkerheds netsikkerhedstjeneste vil således fortsat være forpligtet til at slette data, når formålet med behandlingen er opfyldt, hvis dette sker før den maksimale opbevaringsperiodes udløb. Samtidig vil det generelle princip i den foreslåede § 14 om, at indsamlede personoplysninger

ikke må opbevares på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles, også finde anvendelse på personoplysninger, der behandles af netsikkerhedstjenesten".

Foreningen kan tilslutte sig den foreslåede ordning og de anførte bemærkninger.

Videregivelse af data.
Set i lyset af det nødvendige samarbejde med andre landes it-sikkerhedsmyndigheder samt danske udbydere af offentlige elektroniske kommunikationsnet og -tjenester (teleselskaber) samt andre netsikkerhedstjenester, bemærker foreningen, at disse bestemmelser forekommer naturlige. Det bør dog overvejes, hvorvidt videregivelse af følsomme persondata bør kunne ske i anonymiseret form, medmindre formålet med videregivelsen dermed kompromitteres.

Afsluttende bemærkninger.
Retspolitisk Forening ønsker sammenfattende at bemærke, at en sammenlægning af de hidtidige statslige civile it-sikkerhedsfunktioner (GovCERT) med Forsvarets efterretningstjeneste ud fra en samlet betragtning er betænkelig dels på grund af sikkerhedsopgavernes civile karakter, de med sammenlægningen foreslåede svækkelser af persondatalovens retssikkerhedsgarantier og dels på grund af et stærkt svækket tilsyn.

Såfremt en sammenlægning alligevel findes absolut påkrævet, kan centrets virksomhed formentlig uden de store vanskeligheder opdeles i en militær og civil del, hvor den civile del med visse undtagelser reguleres efter de gældende regler, herunder reglerne om tilsyn i persondataloven.

København, den 3. marts 2014

Leif Hermann
Bestyrelsesmedlem

Bjørn Elmquist
formand

Justitsministeriet
Politi- og Strafferetsafdelingen
Sikkerheds- og Forebyggelseskontoret
Slotholmsgade 10
1216 København K

DATO 4. marts 2014

JOURNAL NR.
RA-2014-510-0033
BEDES ANFØRT VED SVARSKRIVELSER
SAGSBEHANDLER: DRL

RIGSADVOKATEN

FREDERIKSHOLMS KANAL 16
1220 KØBENHAVN K

TELEFON 72 68 90 00
FAX 72 68 90 04

Ved e-mail af 4. februar 2014 (sagsnr. 2013/003214) har Forsvarsministeriet fremsendt udkast til forslag til lov om Center for Cybersikkerhed samt evaluering af GovCERT-loven med anmodning om eventuelle bemærkninger.

I den anledning skal jeg bemærke, at jeg er bekendt med Rigspolitiets bemærkninger af 28. februar 2014 til udkastet (j.nr. 2014-005-39). Jeg kan tilslutte mig, at der i lovforslagets bemærkninger bør medtages en beskrivelse af politiets og anklagemyndighedens kompetence til at behandle sager om mulige strafbare forhold, og at det tydeligt bør fremgå, at sager om mulige strafbare forhold skal behandles af politiet og anklagemyndigheden.

Jeg skal endvidere bemærke, at det som bekendt er besluttet at styrke politiets og anklagemyndighedens indsats mod it-kriminalitet/cyber crime. Der skal i den forbindelse udarbejdes retningslinjer om forholdet mellem politikredsene og Rigspolitiets bistand i disse sager. Retningslinjerne skal bl.a. sikre, at sager om mulige strafbare forhold i overensstemmelse med retsplejelovens regler straks bliver forankret i en politikreds, herunder med henblik på at sikre en entydig placering af ansvaret for kvalitets- og legalitetssikringen i disse sager.

Med venlig hilsen

Ole Hasselgaard

RIGSPOLITIET

POLITI

Justitsministeriet
Sikkerheds- og Forebyggelseskontoret

28. februar 2014
j.nr. 2014-005-39

RIGSPOLITIET

Direktionssekretariatet
Polititorvet 14
1780 København V

Telefon: 3314 8888
Direkte: 4515 2029
Telefax: 4515 0000

Web: www.politi.dk

Ved e-mail af 4. februar 2014 modtog Rigspolitiet en høring fra Forsvarsministeriet over udkast til lovforslag for Center for Cybersikkerhed og udkast til evaluering af GovCERT-loven. I henhold til telefonisk aftale mellem Justitsministeriet og Rigspolitiet af den 5. februar 2014 fremsendes nedenfor Rigspolitiets bemærkninger.

Rigspolitiet skal indledningsvis mere generelt bemærke, at lovforslaget har til formål at fastlægge opgaver og kompetencer for Center for Cybersikkerhed, herunder centerets undersøgelse af hændelser vedrørende brud på informationssikkerheden samt internettrusler. En del af Center for Cybersikkerheds opgaver vil tillige ofte være sager om mistanke om strafbare forhold begået i Danmark, hvilket er politiets kompetence at efterforske. På denne baggrund finder Rigspolitiet det hensigtsmæssigt, såfremt der i bemærkningerne til lovforslaget tilføjes en nærmere beskrivelse af politiets kompetence til at efterforske, herunder at et tæt samarbejde mellem Center for Cybersikkerhed og politiet bl.a. skal sikre understøttelse af politiets efterforskning af mulige strafbare forhold.

Endvidere har Rigspolitiet følgende mere konkrete bemærkninger til udkastet til lovforslag:

Der bør af loven fremgå en pligt for Center for Cybersikkerhed til uden unødigt ophold at foretage anmeldelse af væsentlige sikkerhedshændelser til politiet. Tids-

faktoren kan således være af afgørende betydning for mulighederne for at foretage bevissikring af sagerne.

I bemærkningerne til lovforslagets pkt. 3.1.2., side 13, 3. afsnit, henvises til Center for Cybersikkerheds behov for at undersøge it-udstyr, der har været ramt af angreb, med henblik på at klarlægge angrebsmetoder og -værktøjer. Da der kan være tale om udstyr, som kan indeholde bevismateriale fra en kriminel handling, bør it-udstyret først undersøges af politiet, inden det undersøges nærmere af Center for Cybersikkerhed.

Endvidere fremgår det af bemærkningerne til lovforslagets side 32, 4. afsnit, at Center for Cybersikkerhed sikrer bevismateriale i sager om brud på informationssikkerheden. Da det må antages, at det pågældende bevismateriale eventuelt vil skulle anvendes til brug for en anmeldelse til politiet, bør bevismaterialet derfor sikres efter samråd med politiet, således at bevismaterialet rent faktisk kan anvendes i den videre efterforskning.

Det bemærkes endelig, at de på side 33, 6. afsnit nævnte eksempler på sikkerhedshændelser, er strafbare forhold, som efterforskes af politiet.

Med venlig hilsen

Pernille Breinholdt Mikkelsen
sekretariatschef

RIGSREVISIONEN

Forsvarsministeriet
Holmens Kanal 42
1060 København K

St. Kongensgade 45
1264 København K

Tlf. 33 92 84 00
Fax 33 11 04 15

rr@rigsrevisionen.dk
www.rigsrevisionen.dk

4. marts 2014

Kontor: 13. kontor

J.nr.: 2014-4500-46

Høring over udkast til forslag til lov om Center for Cybersikkerhed samt Evaluering af GovCERT-loven

Forsvarsministeriet har den 4. februar 2014 sendt et udkast til forslag til lov om Center for Cybersikkerhed samt udkast til evaluering af GovCERT-loven i høring (Forsvarsministeriets sagsnummer: 2013/003214).

Rigsrevisionen har ingen bemærkninger til de 2 udkast.

Med venlig hilsen

Sven Dinesen
Souschef, specialkonsulent

4. marts 2014

Forsvarsministeriet
Att.: Peter Heiberg
Holmens Kanal 42
1060 København K
Mail: pah@fmn.dk

Vedr.: Høring over udkast til forslag til lov om Center for Cybersikkerhed.

Rådet for Digital Sikkerhed (RfDS) takker for høringsanmodningen fra Forsvarsministeriet i forbindelse med forslag til lov om Center for Cybersikkerhed.

RfDS finder det positivt, at der nu tages skridt til at etablere et formelt lovgrundlag for oprettelse af Center for Cybersikkerhed (CFCS) samt for videreførelse af GovCERTs opgaver. Det er ligeledes positivt, at der i samme forbindelse etableres et lovgrundlag for MILCERTs virke, som tidligere har været ureguleret. Dette bidrager til gennemsigtighed og forudsigelighed i forhold til CFCS opgaveløsning, og skaber fornøden hjemmel til at løse de opgaver, der knytter sig til undersøgelse og beskyttelse mod cyberangreb.

RfDS har dog en række kommetarer til forslaget af principiel karakter, der knytter sig til beskyttelsen af retssikkerhed og personlig frihed i et demokratisk samfund og til danske virksomheders forretningsinteresser. En række kommentarer knytter derudover an til de konkrete dele af det foreliggende forslag, som RfDS vurderer vil have betydelig effekt på den effektive beskyttelse af borgeres og virksomheders data.

RfDSs kommentarer og opfordringer er uddybet i det følgende og kan opsummeres således:

1. **Retssikkerhed og personlig frihed**

RfDS opfordrer til, at ministeriet revurderer det foreliggende forslag og i stedet finder en organisatorisk løsning, der sikrer, at undersøgelse og forebyggelse af cyberangreb placeres i en forvaltningsmyndighed, der er underlagt almindelige forvaltningsretlige principper for åbenhed, kontrol og indsigt samt retsplejelovens krav om retskendelse ved indgreb i borgernes meddelelseshemmelighed. RfDS finder, at der er et grundlæggende problem i det fremlagte forslag, idet forslagets definition af sikkerhedshændelser er så bred, at selv mindre hændelser vil være begrundelse nok til at opnå adgang til information uden om de almindeligt gældende demokratiske procedurer.

2. **Definition af samfundsvigtige funktioner**

RfDS opfordrer til, at det kun er virksomheder inden for kritisk infrastruktur, som kan tilsluttes CFCSs netssikkerhedstjeneste. Begrebet "kritisk infrastruktur" bør defineres i lovforslagets § 2 og præciseres ved oplistning af virksomhedstyper i de tilhørende bemærkninger.

3. **Konkurrenceforvridning**

RfDS opfordrer til, at CFCSs opgaver afgrænses således, at CFCS ikke medvirker til forvridning af den konkurrence, der i dag består på markedet mellem sikkerhedsvirksomheder, og at CFCS ikke selv

forestår behandling af pakke- og trafikdata på midlertidigt tilsluttede virksomhedsnetværk (§ 6) og af data i eller fra informationssystemer i private virksomheder (§7).

4. Gensidig oplysningspligt

RfDS opfordrer til, at lovforslaget tilføjes en bestemmelse om, at virksomheder har pligt til at orientere CFCS om sikkerhedshændelser og til at stille relevant materiale til rådighed for CFCSs analyser heraf, såfremt det er nødvendigt for at sikre samfundsvigtig informations- og kommunikationsteknologisk infrastruktur. Tilsvarende bør CFCS pålægges pligt til at informere og dokumentere konstaterede sikkerhedshændelser ikke blot mod tilsluttede og midlertidigt tilsluttede virksomheder, men også til de virksomheder, der har været udsat for en sikkerhedshændelse, samt deres brancheforeninger.

5. Behandling af pakkedata

RfDS finder ikke, at der med lovforslaget sikres tilstrækkelig beskyttelse af borgernes og virksomhedernes data, og opfordrer derfor til, at CFCS i det hele adskilles fra Forsvarets Efterretningstjenestes funktionsområde og henlægges til en forvaltningsmyndighed, der er omfattet af persondataloven.

6. Brud på kryptering

RfDS opfordrer til, at adgangen for CFCS til at bryde kryptering gøres betinget af, at der pålægges editionspligt eller at dekryptering gennemtvinges efter forudgående retskendelse. Såfremt det ikke er muligt at indhente retskendelse uden formålet forspildes, må den indhentes efterfølgende, ligesom tilsynsmyndigheden bør orienteres om indgrebet.

7. Blokering af telekommunikation

RfDS opfordrer til, at videregivelse af trafikdata til private udbydere af kommunikationsnet og -tjenester kun sker efter retskendelse. Teleselskaber, der af CFCS på denne måde oplægges blokering, skal orienteres om tidsperioden for blokeringen og sikres, at blokeringen sker på CFCSs ansvar. Teleselskaberne skal ligeledes kunne kompenseres for deres udgifter hertil.

8. Intern videregivelse til FE

RfDS påpeger, at der sker en alvorlig begrænsning af borgernes rettigheder, når al kommunikation mellem borgere/virksomheder og den offentlige sektor potentielt kan gøres til genstand for CFCSs analyser og videregives til FE. RfDS opfordrer derfor til en grundlæggende ændring af lovgrundlaget. I det mindste bør videregivelse til FE reguleres således, at der stilles krav om en konkret vurdering af relevans, nødvendighed og proportionalitet i hvert enkelt tilfælde af intern videregivelse.

9. Videregivelse af data til udlandet

RfDS anbefaler, at lovudkastet udtrykkeligt nævner, at videregivelse kan ske til udenlandske nettjenester og opfordrer til, at videregivelsen til udenlandske nettjenester begrænses til trafikdata, der knytter sig til en sikkerhedshændelse.

10. Slettefrister

RfDS finder det hverken nødvendigt eller proportionalt, at pakkedata kan gemmes i 13 måneder, når de ikke knytter sig til en sikkerhedshændelse, og opfordrer til, at fristen ændres til 30 dage. I forhold til videregivelse af trafikdata til teleudbydere og ved videregivelse til myndigheder i udlandet bør der stilles krav om sletning, når formålet med behandlingen er opfyldt, dog senest efter henholdsvis tre år for data med tilknytning til en sikkerhedshændelse og 30 dage for data uden en sådan tilknytning.

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

11. Sagkyndigt tilsyn

RfDS opfordrer til, at det sikres, at den fornødne sagkundskab inden for it-revision og it-sikkerhed er til stede i Tilsynet med Efterretningstjenesterne eller en anden relevant tilsynsmyndighed tillige med repræsentation af relevante juridiske fagområder, herunder borgernes grundrettigheder.

Uddybende kommentarer

1. Retssikkerhed og personlig frihed

RfDS har fuld forståelse for og anerkender nødvendigheden af at styrke sikkerheden i den danske informations- og kommunikationsteknologiske infrastruktur mod cyberangreb fra såvel stater som grupper og enkeltpersoner, der bruger internettet til at spionere mod danske myndigheder, virksomheder og borgere eller anrette skader i deres it-systemer.

RfDS anser det dog for helt afgørende, at den organisation, der skal varetage funktionen som Danmarks nationale it-sikkerhedsmyndighed, bliver etableret og drives i overensstemmelse med de principper og værdier, vores demokrati bygger på. Det er i den sammenhæng helt afgørende effektivt at beskytte borgernes retssikkerhed og personlige frihed mod unødvendig og uproportional overvågning og indsigt i personlige data.

Statens interesse i overvågning kan aldrig tilsidesætte borgernes grundrettigheder, men må ses som en undtagelse, der kun kan iværksættes, hvis der foreligger grunde, der vejer tungere end hensynet til den enkelte borger og er nødvendige og proportionale i forhold til det formål, indgrebet søger at opfylde. Et optimalt beskyttelsesniveau i forhold til sikkerhedshændelser må derfor ikke søges opnået på bekostning af borgernes grundrettigheder. Det bemærkes i denne sammenhæng, at forslagets definition af sikkerhedshændelser er så bred, at selv mindre hændelser vil være begrundelse nok til, at der kan opnås adgang til information behandlet i netværk og it-systemer hos tilsluttede og midlertidigt tilsluttede myndigheder og virksomheder uden retskendelse. Det er ligeledes afgørende, at redskaber og indsatser til at undersøge og forebygge sikkerhedshændelser ikke indføres på grundlag af frivilligt indgåede aftaler mellem private virksomheder og staten, hvis indhold reelt udgør en tilsidesættelse af de retssikkerhedsgarantier, der er indlejret i dansk lovgivning.

Grundloven, retsplejeloven, EU traktaten og den Europæiske Menneskerettighedskonvention sikrer alle et sådant værn af borgerne.

I lyset heraf finder RfDS det problematisk, at en række opgaver, der hidtil er varetaget af myndigheder, der er underlagt krav om åbenhed, kontrol og indsigt samt de principper, der er indlejret i forvaltningsloven, offentlighedsloven og persondataloven samt retsplejelovens krav om indhentelse af retskendelse før brud på meddelelseshemmeligheden, med lovforslaget flyttes til en lukket del af den offentlige forvaltning i form af Forsvarets Efterretningstjeneste, der i vidt omfang er fritaget for opfyldelse af disse krav.

Det gælder de opgaver, der tidligere blev varetaget af IT- og Telestyrelsen, herunder GovCERT funktionen og informationssikkerhed og beredskab på teleområdet.

RfDS opfordrer til, at ministeriet revurderer det foreliggende forslag og i stedet finder en organisatorisk løsning, der sikrer, at undersøgelse og forebyggelse af cyberangreb placeres i en forvaltningsmyndighed, der er underlagt almindelige forvaltningsretlige principper for åbenhed, kontrol og indsigt samt retsplejelovens krav om retskendelse ved indgreb i borgernes

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr : 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

meddelelseshemmelighed. RfDS finder, at der er et grundlæggende problem i det fremlagte forslag, idet forslagets definition af sikkerhedshændelser er så bred, at selv mindre hændelser vil være begrundelse nok til at opnå adgang til information uden om de almindeligt gældende demokratiske procedurer.

2. Definition af "samfundsvigtige funktioner"
Med lovforslagets § 1 og § 3, stk. 3 vil CFCS opgaver omfatte undersøgelser og imødegåelse af sikkerhedshændelser i tilsluttede virksomheder, der er beskæftiget med samfundsvigtige funktioner. Dette er en udvidelse i forhold til GovCERT-lovens § 2, der afgrænsede netsikkerhedtjenesten til kritisk infrastruktur.

Af lovforslagets bemærkninger fremgår, at det reelt vil være en ganske stor del af det private erhvervsliv, der kan tilslutte sig CFCS netsikkerhedstjeneste. Det anføres således, at samfundsvigtige funktioner omfatter: "sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet ... medicinalvirksomheder, fødevarevirksomheder, virksomheder, der leverer vigtige komponenter til Forsvaret, og virksomheder, der varetager driften af administrative it-systemer for det offentlige".

De oplistede virksomhedstyper er alene nævnt som eksempler i bemærkningerne. Afgrænsningen af relevante virksomheder bør angives præcist og knyttes til en definitionsbestemmelse af "samfundsvigtige funktioner" i lovforslagets § 2, for så vidt at denne udvidelse fastholdes.

RfDS opfordrer til, at det kun er virksomheder inden for kritisk infrastruktur, som kan tilsluttes CFCS netssikkerhedstjeneste. Begrebet "kritisk infrastruktur" bør defineres i lovforslagets § 2 og præciseres ved oplistning af virksomhedstyper i de tilhørende bemærkninger.

3. Konkurrenceforvridning
Med udvidelsen af CFCSs funktionsområde til at omfatte sikkerhedsniveauet i virksomheder med samfundsvigtige funktioner og med mulighed for tilslutning af sådanne virksomheder til CFCSs netsikkerhedstjeneste, går denne i direkte konkurrence med private udbydere af sikkerhedstjenester.

Flere sikkerhedsvirksomheder har f.eks. et system af prober til at opsamle data og analysere sikkerhedshændelser på det globale internet, svarende til hvad CFCS netsikkerhedstjeneste har på den danske del af internettet. De pågældende virksomheder har selv status af at være CERTer eller CSIRTer og indgår derfor i CERT-CC samarbejdet med deres data.

Adgangen for CFCS efter forslagets § 6 og 7 til at behandle data ved begrundet mistanke om en sikkerhedshændelse udgør en tilsvarende forvridning af konkurrencesituationen. Der er således et større antal private aktører, som allerede påtager sig at levere sådanne services på markedsvilkår.

At være i konkurrence med sådanne virksomheder synes ikke at være foreneligt med CFCSs formål og forvrider konkurrencen på markedet. Hvis der sker en sådan forvridning, må det antages at påvirke den samlede kvalitet af de sikkerhedsydelser som er tilgængelige for de relevante aktører.

RfDS opfordrer til, at CFCSs opgaver afgrænses således, at CFCS ikke medvirker til forvridning af den konkurrence, der i dag består på markedet mellem sikkerhedsvirksomheder. CFCS bør derfor ikke selv forestå behandling af pakke- og trafikdata på midlertidigt tilsluttede netværk (§ 6) og af data i eller fra informationssystemer (§7), men overlade det til private sikkerhedsvirksomheder.

Radet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

4. Gensidig oplysningspligt
RfDS anerkender behovet for at tilvejebringe nødvendige oplysninger om sikkerhedshændelser, der kan indgå i CFCS arbejde med at sikre informations- og kommunikationsteknologisk infrastruktur. Ved inddragelse af private aktører, jfr. punkt 2 ovenfor, bør en sådan videnstilførsel sikres gennem en forpligtelse for virksomheder med samfundsvigtige funktioner til at oplyse CFCS om sikkerhedshændelser og til at stille data til rådighed for CSFC, såfremt det er nødvendigt for at sikre infrastrukturen.

For at sikre effektiv forebyggelse i tilsluttede og midlertidigt tilsluttede virksomheder, bør der tilsvarende pålægges CFCS en forpligtelse til at orientere den enkelte virksomhed eller sektorens brancheorganisation om sikkerhedshændelser og til at fremlægge relevant dokumentation for angrebet.

RfDS opfordrer til, at lovforslaget tilføjes en bestemmelse om, at virksomheder har pligt til at orientere CFCS om sikkerhedshændelser og til at stille relevant materiale til rådighed for CFCS analyser heraf, såfremt det er nødvendigt for at sikre samfundsvigtig informations- og kommunikationsteknologisk infrastruktur. Tilsvarende bør CFCS pålægges pligt til at informere og dokumentere konstaterede sikkerhedshændelser ikke blot til tilsluttede og midlertidigt tilsluttede virksomheder, men til de virksomheder, der har været udsat for en sikkerhedshændelse, samt deres brancheforeninger.

5. Adgang til pakkedata
RfDS har fuld forståelse for, at CFCS fremtidige analyser og undersøgelser af cyberangreb og forsøg på sådanne er afhængig af adgang til såvel trafikdata som pakkedata. Pakkedata omfatter indhold af fx mails og vedhæftede filer og vil derfor give indsigt i såvel personlige som personfølsomme oplysninger tillige med oplysninger om beskyttelsesværdige forretningshemmeligheder.

Som udgangspunkt er det derfor positivt, at lovforslagets § 15 fastlår, at analyse af pakkedata indhentet i medfør af §§ 4, 6 og 7 kun må "finde sted ved begrundet mistanke om en sikkerhedshændelse og kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen" (svarende til bestemmelsen i GovCERT-lovens § 4, stk. 1).

RfDS finder dog, at det er af afgørende betydning for den effektive beskyttelse af borgeres og virksomheders data, at CFCS – efter indhentet retskendelse til adgang til netværk og it-systemer, jfr. ovenfor under punkt 1 – foretager sine analyser af dette materiale i overensstemmelse med persondataloven.

Behovet for at fastsætte disse krav understreges af, at CFCS gennem de nuværende GovCERT prober vil få adgang til næsten al kommunikation mellem borgerne/virksomheder og staten, ligesom de på længere sigt får adgang til næsten al kommunikation mellem borger/virksomheder og hele den offentlige sektor m.v.

RfDS bemærker hertil, at der med ophævelse af GovCert-loven vil ske en væsentlig forringelse af databeskyttelsen. Mens GovCERT-lovens § 5 præciserede, at GovCERT-funktionen alene var undtaget persondatalovens § 35, vil CFCS med sin placering under FE generelt være undtaget hele persondataloven, jf. CFCS-loven § 8, stk. 1 og persondataloven § 2, stk. 11.

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr : 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

Med lovforslaget skrives alene dele af persondatalovens principper ind i CFCS-loven. Således svarer §§ 9-14 og § 18 i CFCS-loven til persondatalovens §§ 5, 6, 7, 8 og dele af § 41. Men følgende vigtige bestemmelser for opretholdelse af effektiv databeskyttelse er udeladt:

- der skal ikke indhentes tilladelse fra Tilsynet med Efterretningstjenesterne i principielle sager hvor der behandles personoplysninger, eller ske underretning til EU kommissionen, jf. f.eks. persondataloven § 7, stk. 7.
- kataloget over registreredes rettigheder i persondatalovens §§ 28-40 om bl.a. underretning og indsigtsadgang opretholdes ikke.
- krigsreglen i persondatalovens § 41, stk. 4 om bortskaffelse eller tilintetgørelse af oplysninger fra den offentlige forvaltning i tilfælde af krig eller lignende forhold er ikke indføjet i CFCS-loven.

RfDS bemærker endvidere, at evalueringen af GovCERTs virke, som Forsvarsministeren skal give Folketinget i henhold til GovCERT-lovens § 9, og som foreligger i udkast fra januar 2014, ikke indeholder vurderinger, der viser et fagligt behov for at udvide undtagelserne fra persondataloven.

I lyset af EMRK art. 8 og EU traktatens charter om grundrettigheders art. 8 skal et indgreb i borgernes grundrettighed til persondatabeskyttelse være nødvendigt i et demokratisk samfund og proportionalt. I proportionalitetsvurderingen skal indgå en rimelighedsvurdering af, om de samfundsmæssige interesser i at håndtere sikkerhedshændelser for offentlige myndigheder er så tungtvejende, at de kan tilsidesætte hensynet til den enkelte borgers privatlivs- og persondatabeskyttelse.

RfDS finder ikke, der med lovforslaget sikres tilstrækkelig beskyttelse af borgernes og virksomhedernes data, og opfordrer derfor til, at CFCSs virksomhed i det hele adskilles fra Forsvarets Efterretningstjenestes funktionsområde og henlægges til en forvaltningsmyndighed, der er omfattet af persondataloven.

6. Brud på kryptering

Med CFCS-loven skabes der lovhjemmel til at CFCS får adgang til at bryde kryptering (bemærkninger til lovforslagets enkelte bestemmelser, p. 37). Dette udgør en markant udvidelse af datagrundlaget i forhold til dét, GovCERT var tillagt efter GovCERT-loven.

Det bemærkes, at formuleringen om at bryde kryptering ikke umiddelbart giver mening, da det betyder at finde frem til beskeden uden at kende nøglen. Dette er i praksis umuligt, med mindre der er tale om kryptering som ikke er korrekt designet eller ikke har tilstrækkelig styrke. For så vidt der er tale om korrekt designet kryptering, antager RfDS derfor, at det som menes, er at man pålægger modtageren til at udlevere dekrypteringsnøglen.

RfDS anerkender, at cyberangreb og forsøg på sådanne ofte skjules ved anvendelse af kryptering, men i lyset af, at borgere og virksomheder ofte bruger kryptering til at særligt fortrolige data, består der et ekstra sikkerheds- og beskyttelseshensyn, som lovudkastet ikke forholder sig til. RfDS opfordrer derfor til, at CFCS ikke tildeles beføjelser til at forlange dekrypteringsnøgler udleveret, men at adgang til krypterede data i stedet sikres ved en procedure svarende til retsplejelovens regler om beslaglæggelse og edition.

RfDS opfordrer til, at adgangen for CFCS til at bryde kryptering gøres betinget af, at der pålægges editionspligt eller at dekryptering gennemtvinges efter forudgående retskendelse. Såfremt det ikke er

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

muligt at indhente retskendelse uden formålet forspildes, må den indhentes efterfølgende, ligesom tilsynsmyndigheden bør orienteres om indgrebet.

7. Blokering af telekommunikation
RfDS anerkender, at CFCS kan have behov for at videregive trafikdata til teleselskaberne for fx at opnå blokering af IP-adresser, der mistænkes for anvendelse til cyberangreb. Med CFCS-lovforslaget skabes der hjemmel hertil med § 16, når videregivelsen er nødvendig for udførelsen af netsikkerhedstjenestens opgaver.

Beskyttelsen af samfundsvigtige funktioner gennem blokering eller lignende bør imidlertid kun ske på baggrund af en retskendelse og en klar præcisering af ansvaret for det af CFCS pålagte indgreb i telekommunikationen. Lovforslaget bør derfor tilføjes en bestemmelse om indhentelse af en retskendelse, der præciserer, hvilke adresser eller numre, blokeringen angår og hvilket tidsrum blokeringen eller tilsvarende indgreb skal opretholdes. Det bør desuden overvejes at kompensere teleselskaberne for den økonomiske byrde, det vil være at implementere og fjerne en pålagt blokering.

RfDS opfordrer til, at videregivelse af trafikdata til private udbydere af kommunikationsnet og -tjenester kun sker efter retskendelse. Teleselskaber, der af CFCS på denne måde oplægges blokering, skal orienteres om tidsperioden for blokeringen og sikres, at blokeringen sker på CFCSs ansvar. Teleselskaberne skal ligeledes kunne kompenseres for deres udgifter hertil.

8. Intern videregivelse af data til FE
RfDS bemærker, at Forsvarets Efterretningstjeneste (FE) får adgang til GovCERT data, herunder pakkedata, og derfor vil kunne benytte disse data inden for de rammer, der er fastsat i FE-loven.

Det fremgik af GovCERT-loven § 6, stk. 2, at "Pakkedata, der knytter sig til en sikkerhedshændelse, kan videregives til Forsvarets Efterretningstjenestes militære CERT, hvor IT- og Telestyrelsen skønner det nødvendigt for at beskytte nationale digitale infrastrukturer mod sikkerhedsmæssige trusler".

Med forslag til CFCS-lov fjernes denne beskyttelse, fordi CFCS indgår som en enhed i Forsvarets Efterretningstjeneste. Det fremgår således af de almindelige bemærkninger, s. 26, at "En sådan intern udveksling af data har efter oprettelsen af Center for Cybersikkerhed ikke længere karakter af en videregivelse, og den interne udveksling af data i Forsvarets Efterretningstjeneste er... ikke længere reguleret i lovforslaget".

Det fremgår endvidere i de almindelige bemærkninger s. 26, at "Forsvarsministeriet vil imidlertid med lov om Center for Cybersikkerheds ikrafttræden udstede administrative retningslinjer, der sikrer, at den interne udveksling af oplysninger mellem Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste også fremadrettet sker med respekt for retssikkerheden og den personlige frihed".

RfDS finder, at det er en uheldig konsekvens af CFCSs placering i FE, at der åbnes for udveksling af data med FE uden iagttagelse af nødvendige retssikkerhedshensyn. CFCS opgaver rummer såvel militær varslingstjeneste (MilCERT) og statslig varslingstjeneste (GovCERT), og i tilknytning hertil civile opgaver i form af netsikkerhedstjeneste for kommuner, regioner og virksomheder samt informationssikkerhed og bredskab på teleområdet. Data fra disse opgaver ligger ikke inden for det område, som FE i medfør af FE-loven, er bemyndiget til at udføre. Der er derfor forøget risiko for, at

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

data fra civile indretninger og systemer gøres til genstand for analyser eller kobles sammen med oplysninger, der hidrører fra FEs sædvanlige opgaver og som sådan er koblet til efterretningsopgaver uden for Danmarks grænser.

Det udgør efter RfDSs opfattelse en alvorlig indskrænkning af de grundlæggende rettigheder, som borgerne nyder efter såvel grundloven, retsplejeloven, EMRK og EU traktaten, da al kommunikation mellem borgere/virksomheder og den offentlige sektor potentielt vil kunne gøres til genstand for CFSCs analyser og videregives til FE.

RfDS opfordrer derfor til en grundlæggende ændring af lovgrundlaget for CFCS, herunder en adskillelse af CFCS fra FE, der sikrer at CFCS udfører deres opgaver med respekt for forvaltningsloven, offentlighedsloven og persondataloven, og med iagttagelse af de retssikkerhedsgarantier, der er indeholdt i retsplejeloven i tilknytning til indgreb i meddelelseshemmeligheden.

I tilfælde af, at lovforslaget fremlægges i sin nuværende form, opfordrer RfDS til, at der straks efter vedtagelsen af loven, udstedes administrative retningslinjer, der indeholder krav om konkret vurdering af relevans, nødvendighed og proportionalitet i alle sager om videregivelse af pakkedata fra CFCS til FE.

RfDS påpeger, at der sker en alvorlig begrænsning af borgernes rettigheder, når al kommunikation mellem borgere/virksomheder og den offentlige sektor potentielt kan gøres til genstand for CFCSs analyser og videregives til FE. RfDS opfordrer derfor til en grundlæggende ændring af lovgrundlaget. I det mindste bør videregivelse til FE reguleres således, at der stilles krav om en konkret vurdering af relevans, nødvendighed og proportionalitet i hvert enkelt tilfælde af intern videregivelse.

9. Videregivelse af data til udlandet

RfDS anerkender nødvendigheden af at CFCS kan have behov for at videregive trafikdata til andre landes CERTer og ikt-myndigheder i forbindelse med grænseoverskridende cyberangreb.

Forslaget til CFCS-loven indeholder hjemmel hertil i §16, nr. 2, hvoraf det fremgår, at "trafikdata videregives til... andre netsikkerhedstjenester". Kvalitetskrav til lovgrundlag, der griber ind i borgernes beskyttede grundrettigheder, omfatter krav om klarhed i lovhjemlen og forudsigelighed i forhold til dens anvendelse. De almindelige bemærkningers angivelse af behovet for at videregive data til udenlandske nettjenester bør derfor indskrives direkte ind i lovforslagets § 16 nr. 2, således at det klart fremgår at videregivelse kan ske til "udenlandske nettjenester".

RfDS opfordrer derudover til, at der lægges begrænsninger på omfanget af trafikdata, som kan videregives til udlandet. En bestemmelse herom bør knytte an til bestemmelsen i lovforslagets § 2, nr. 1, så det sikres, at det udelukkende er trafikdata, der knytter sig til en sikkerhedshændelse, der videregives til udenlandske nettjenester. Alternativt bør § 16, nr. 2 alene henvise til data omfattet af § 6 og § 7, således at data, der er behandlet med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet, ikke kan videregives til udlandet.

RfDS anbefaler, at lovudkastet udtrykkeligt nævner, at videregivelse kan ske til udenlandske nettjenester og opfordrer til, at videregivelsen til udenlandske nettjenester begrænses til trafikdata, der knytter sig til en sikkerhedshændelse.

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk

10. Slettefrister

Med CFCS-loven ændres der betydeligt i slettefristerne. Trafik- og pakkedata vil efter lovforslaget blive behandlet ens. Det betyder, at data, der knytter sig til en sikkerhedshændelse, må opbevares i højst tre år, mens data, der ikke knytter sig til en sikkerhedshændelse, må opbevares i 13 måneder. Efter GovCERT-lovens § 4, stk. 3, nr. 2 var slettefristen for sidstnævnte type data 14 dage.

Yderligere slås det i CFCS-loven, § 4, stk. 4 fast, at der ikke stilles krav om sletning for data, som videregives. Det må forstås således, at det også omfatter data, der videregives til udlandet.

RfDS finder det hverken nødvendigt eller proportionalt, at pakkedata kan gemmes i 13 måneder, når de ikke knytter sig til en sikkerhedshændelse, og opfordrer til, at fristen ændres til 30 dage. I forhold til videregivelse af trafikdata til teleudbydere og ved videregivelse til myndigheder i udlandet bør der stilles krav om sletning, når formålet med behandlingen er opfyldt, dog senest efter henholdsvis tre år for data med tilknytning til en sikkerhedshændelse og en måned for data uden en sådan tilknytning.

11. Sagkyndigt tilsyn

I lyset af den foreslåede placering af CFCS i FE finder RfDS det naturligt at nedlægge Tilsynet med GovCERT og overlade opgaven til Tilsynet med Efterretningstjenesterne. For effektivt at sikre borgernes og virksomhedernes data bør det dog foretrækkes, at CFCS opgaver og tilsyn placeres i det almindelige forvaltningsretlige system, jfr. også punkt 1 ovenfor.

Tilsynet med GovCERT skulle i henhold til GovCERT-loven §7, stk. 2 kunne præstere juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab. Tilsynet med CFCS bliver i henhold til CFCS-loven, kapitel 9, Tilsynet med Efterretningstjenesterne. Men i PET-lovens kapitel 9 findes der ikke tilsvarende krav til sagkundskaben hos dem, der udpeges til Tilsynet. Der er derfor en risiko for, at tilsynet vil mangle tilstrækkelig faglig kompetence til at føre tilsyn med CFCS.

RfDS opfordrer til, at det sikres, at den fornødne sagkundskab inden for it-revision og it-sikkerhed er til stede i Tilsynet med Efterretningstjenesterne eller i en tilsynsmyndighed i den almindelige forvaltning tillige med repræsentation af relevante juridiske fagområder, herunder om borgernes grundrettigheder.

Med venlig hilsen

Birgitte Kofod Olsen
Formand

Lars Stig Jørgensen
Næstformand

Rådet for Digital Sikkerhed, Toldbodgade 12, 1253 København K, Danmark - CVR-nr.: 34757488
Web: www.digitalsikkerhed.dk Mail: info@digitalsikkerhed.dk